

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference FH990804PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP99/06312	International filing date (<i>day/month/year</i>) 27 August 1999 (27.08.99)	Priority date (<i>day/month/year</i>) 22 September 1998 (22.09.98)
International Patent Classification (IPC) or national classification and IPC G07F 7/10		
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 10 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 06 April 2000 (06.04.00)	Date of completion of this report 22 September 2000 (22.09.2000)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP99/06312

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

- ☒ the international application as originally filed.
- ☒ the description, pages 1,2,4-20, as originally filed,
pages _____, filed with the demand,
pages 3,3a-3b, filed with the letter of 02 August 2000 (02.08.2000),
pages _____, filed with the letter of _____.
- ☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-18, filed with the letter of 02 August 2000 (02.08.2000),
Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 1/4-4/4, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP 99/06312

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims		NO
Inventive step (IS)	Claims	1-18	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following documents:

D1: EP-A-0 313 967 (GAO GES AUTOMATION ORG) 3 May 1989 (1989-05-03)

D2: EP-A-0 654 919 (SIEMENS AG) 24 May 1995 (1995-05-24)

D3: W. RANKL & W. EFFING: 'Handbuch der Chipkarten' 10 February 1998 (1998-02-10), CARL HANSER VERLAG, MÜNCHEN WIEN XP002127583 022759.

The essential difference between the concept of D1 and the concept of the invention consists in the fact that, according to D1 the individual characterising data in the memory (53) is always the same, irrespective of the random number stored in the card (51). In the invention, however, it is essential that the operational data of the circuit also depends on the input data of the circuit. Document D1 does not disclose a device for determining the operational data of the electronic circuit, said data being influenced by an operation of the electronic circuit, when the electronic circuit executes the algorithm. Moreover, in D1 the individual stored data is not dependent on the input

data, that is the random number, which is transmitted from block Z in Figure 11 to block RN. Consequently, document D1 also fails to disclose a device for determining the operational data of the electronic circuit (the operational data of the device (60) in Figure 11 is not determined; the memory (52) is not an element that generates output data from the card depending on input data in the card). Furthermore, D1 does not disclose the fact that the algorithm, which is executed by the electronic circuit, uses the determined operational data of the electronic circuit, since such operational data of the electronic circuit is not even determined.

Proceeding from D1, the invention addresses the problem of developing a concept for the improved protection of electronic circuits and therefore of developing a secure method for authenticating such electronic circuits and a secure method for authorising an owner of such electronic circuits.

This problem is solved as per the invention by a device according to Claim 1 and a method according to Claims 17 or 18.

The solution defined in the independent claims involves an inventive step: unlike in D1, the invention does not use the individual characterising data of just any electronic circuit, but rather the operational data of the electronic circuit which generates output data depending on the input data. The concept as per the invention dispenses with the storing of characterising data in a central processor.

The teaching of D1 differs from the solution as per the invention in that in D1 the individual characterising data in the memory is always the same and can therefore be stored at the beginning, whereas according to the invention, the operational data depends on the input data and therefore a single storage of the operational data would not make any sense. D2 and D3 point further away from the subject matter of the present invention than D1. Although these documents specify different authentication procedures between a transmitter and a receiver, they do not suggest using the technological operational patterns of output data from a card that is to be authorised.

There are no objections concerning industrial applicability.

Consequently, independent Claims 1, 17 and 18 would appear to meet the criteria for novelty, inventive step and industrial applicability stipulated in PCT Article 33(1). Claims 2-16 concern advantageous configurations and therefore also satisfy said criteria.

It is the applicant's opinion that delimitation over D1 would lead to a claim that would be difficult to understand and therefore the one-part form has been used for Claim 1. Since it is sufficiently clear from the detailed discussion of D1 in the description which features of Claim 1 are already known from the prior art, in line with the PCT Guidelines PCT/GL/3, Chapter III-2.3a, the use of the two-part form under PCT Rule 5.1(a)(ii) is not required in this case.

PATENT COOPERATION TREATY

PCT

INFORMATION CONCERNING ELECTED
OFFICES NOTIFIED OF THEIR ELECTION

(PCT Rule 61.3)

From the INTERNATIONAL BUREAU

To:

SCHOPPE, Fritz
 Schoppe, Zimmermann & Stöckeler
 Postfach 71 08 67
 D-81458 München
 ALLEMAGNE

Date of mailing (day/month/year) 16 May 2000 (16.05.00)		IMPORTANT INFORMATION	
Applicant's or agent's file reference FH990804PCT			
International application No. PCT/EP99/06312	International filing date (day/month/year) 27 August 1999 (27.08.99)	Priority date (day/month/year) 22 September 1998 (22.09.98)	
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. et al			

- The applicant is hereby informed that the International Bureau has, according to Article 31(7), notified each of the following Offices of its election:
 EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE
 National : CA, US
- The following Offices have waived the requirement for the notification of their election; the notification will be sent to them by the International Bureau only upon their request:
 None
- The applicant is reminded that he must enter the "national phase" before the expiration of 30 months from the priority date before each of the Offices listed above. This must be done by paying the national fee(s) and furnishing, if prescribed, a translation of the international application (Article 39(1)(a)), as well as, where applicable, by furnishing a translation of any annexes of the international preliminary examination report (Article 36(3)(b) and Rule 74.1).

 Some offices have fixed time limits expiring later than the above-mentioned time limit. For detailed information about the applicable time limits and the acts to be performed upon entry into the national phase before a particular Office, see Volume II of the PCT Applicant's Guide.

 The entry into the European regional phase is postponed until 31 months from the priority date for all States designated for the purposes of obtaining a European patent.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer: F. Baechler Telephone No. (41-22) 338.83.38
--	---

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL BUREAU

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:

SCHOPPE, Fritz
Schoppe, Zimmermann & Stöckeler
Postfach 71 08 67
D-81458 München
ALLEMAGNE

Date of mailing (day/month/year) 30 March 2000 (30.03.00)		IMPORTANT NOTICE	
Applicant's or agent's file reference FH990804PCT			
International application No. PCT/EP99/06312	International filing date (day/month/year) 27 August 1999 (27.08.99)	Priority date (day/month/year) 22 September 1998 (22.09.98)	
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. et al			

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:

US

In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:

CA,EP

The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
30 March 2000 (30.03.00) under No. WO 00/17826

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, a demand for international preliminary examination must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

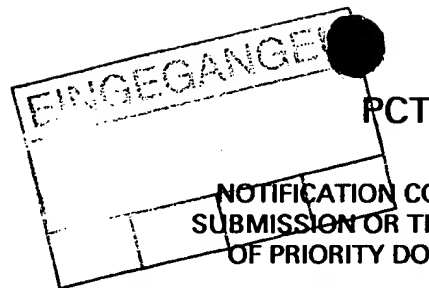
REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the national phase, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer J. Zahra Telephone No. (41-22) 338.83.38
--	---

PATENT COOPERATION TREATY



(PCT Administrative Instructions, Section 411)

From the INTERNATIONAL BUREAU

To:

SCHOPPE, Fritz
Schoppe, Zimmermann & Stöckeler
Postfach 71 08 67
D-81458 München
ALLEMAGNE

Date of mailing (day/month/year) 02 December 1999 (02.12.99)	
Applicant's or agent's file reference FH990804PCT ✓	IMPORTANT NOTIFICATION
International application No. PCT/EP99/06312 ✓	International filing date (day/month/year) 27 August 1999 (27.08.99) ✓
International publication date (day/month/year) Not yet published	Priority date (day/month/year) 22 September 1998 (22.09.98) ✓
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
3. An asterisk(*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, the attention of the applicant is directed to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
4. The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, the attention of the applicant is directed to Rule 17.1(c) which provides that the designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

<u>Priority date</u>	<u>Priority application No.</u>	<u>Country or regional Office or PCT receiving Office</u>	<u>Date of receipt of priority document</u>
22 Sept 1998 (22.09.98)	198 43 424.3	DE	24 Nove 1999 (24.11.99)

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No. (41-22) 740.14.35	Authorized officer G. Bähr Telephone No. (41-22) 338.83.38
--	--

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

SCHOPPE, Fritz
Schoppe, Zimmermann & Stockeler
Postfach 71 08 67
D-81458 München
ALLEMAGNE

EINGEGANGEN			
15.11.1999			

Date of mailing (day/month/year) 03 November 1999 (03.11.99)	
Applicant's or agent's file reference FH990804PCT ✓	IMPORTANT NOTIFICATION
International application No. PCT/EP99/06312 ✓	International filing date (day/month/year) 27 August 1999 (27.08.99) ✓

1. The following indications appeared on record concerning:

☒ the applicant
 ☒ the inventor
 ☐ the agent
 ☐ the common representative

Name and Address

OELMAIER, Florian
Gründlacher Strasse 15
D-91058 Erlangen
Germany

State of Nationality

DE

State of Residence

DE

Telephone No.

Facsimile No.

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person
 ☐ the name
 ☒ the address
 ☐ the nationality
 ☐ the residence

Name and Address

OELMAIER, Florian ✓
Hirtenstrasse 5 ✓
D-85386 Eching ✓
Germany ✓

State of Nationality

DE ✓

State of Residence

DE ✓

Telephone No.

Facsimile No.

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office
 ☐ the designated Offices concerned
☒ the International Searching Authority
 ☐ the elected Offices concerned
☐ the International Preliminary Examining Authority
 ☐ other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

G. Bähr

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF RECEIPT OF RECORD COPY

(PCT Rule 24.2(a))

From the INTERNATIONAL BUREAU

To:

SCHOPPE, Fritz
Schoppe, Zimmermann & Stöckeler
Postfach 71 08 67
D-81458 München
ALLEMAGNE

Date of mailing (day/month/year) 25 October 1999 (25.10.99)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference FH990804PCT	International application No. PCT/EP99/06312 ✓

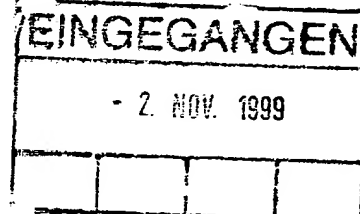
The applicant is hereby notified that the International Bureau has received the record copy of the international application as detailed below.

Name(s) of the applicant(s) and State(s) for which they are applicants:

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (for all
designated States except US) ✓
OELMAIER, Florian et al (for US) ✓

International filing date : 27 August 1999 (27.08.99) ✓
Priority date(s) claimed : 22 September 1998 (22.09.98) ✓
Date of receipt of the record copy
by the International Bureau : 08 October 1999 (08.10.99)
List of designated Offices :

EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE
National : CA, US ✓



ATTENTION

The applicant should carefully check the data appearing in this Notification. In case of any discrepancy between these data and the indications in the international application, the applicant should immediately inform the International Bureau.

In addition, the applicant's attention is drawn to the information contained in the Annex, relating to:

- ☒ time limits for entry into the national phase
- ☒ confirmation of precautionary designations
- ☒ requirements regarding priority documents

A copy of this Notification is being sent to the receiving Office and to the International Searching Authority.

<p>The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland</p> <p>Facsimile No. (41-22) 740.14.35</p>	<p>Authorized officer:</p> <p>G. Bähr </p> <p>Telephone No. (41-22) 338.83.38</p>
---	---

INFORMATION ON TIME LIMITS FOR ENTERING THE NATIONAL PHASE

The applicant is reminded that the "national phase" must be entered before each of the designated Offices indicated in the Notification of Receipt of Record Copy (Form PCT/IB/301) by paying national fees and furnishing translations, as prescribed by the applicable national laws.

The time limit for performing these procedural acts is **20 MONTHS** from the priority date or, for those designated States which the applicant elects in a demand for international preliminary examination or in a later election, **30 MONTHS** from the priority date, provided that the election is made before the expiration of 19 months from the priority date. Some designated (or elected) Offices have fixed time limits which expire even later than 20 or 30 months from the priority date. In other Offices an extension of time or grace period, in some cases upon payment of an additional fee, is available.

In addition to these procedural acts, the applicant may also have to comply with other special requirements applicable in certain Offices. It is the applicant's responsibility to ensure that the necessary steps to enter the national phase are taken in a timely fashion. Most designated Offices do not issue reminders to applicants in connection with the entry into the national phase.

For detailed information about the procedural acts to be performed to enter the national phase before each designated Office, the applicable time limits and possible extensions of time or grace periods, and any other requirements, see the relevant Chapters of Volume II of the PCT Applicant's Guide. Information about the requirements for filing a demand for international preliminary examination is set out in Chapter IX of Volume I of the PCT Applicant's Guide.

GR and ES became bound by PCT Chapter II on 7 September 1996 and 6 September 1997, respectively, and may, therefore, be elected in a demand or a later election filed on or after 7 September 1996 and 6 September 1997, respectively, regardless of the filing date of the international application. (See second paragraph above.)

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

CONFIRMATION OF PRECAUTIONARY DESIGNATIONS

This notification lists only specific designations made under Rule 4.9(a) in the request. It is important to check that these designations are correct. Errors in designations can be corrected where precautionary designations have been made under Rule 4.9(b). The applicant is hereby reminded that any precautionary designations may be confirmed according to Rule 4.9(c) before the expiration of 15 months from the priority date. If it is not confirmed, it will automatically be regarded as withdrawn by the applicant. There will be no reminder and no invitation. Confirmation of a designation consists of the filing of a notice specifying the designated State concerned (with an indication of the kind of protection or treatment desired) and the payment of the designation and confirmation fees. Confirmation must reach the receiving Office within the 15-month time limit.

REQUIREMENTS REGARDING PRIORITY DOCUMENTS

For applicants who have not yet complied with the requirements regarding priority documents, the following is recalled.

Where the priority of an earlier national, regional or international application is claimed, the applicant must submit a copy of the said earlier application, certified by the authority with which it was filed ("the priority document") to the receiving Office (which will transmit it to the International Bureau) or directly to the International Bureau, before the expiration of 16 months from the priority date, provided that any such priority document may still be submitted to the International Bureau before that date of international publication of the international application, in which case that document will be considered to have been received by the International Bureau on the last day of the 16-month time limit (Rule 17.1(a)).

Where the priority document is issued by the receiving Office, the applicant may, instead of submitting the priority document, request the receiving Office to prepare and transmit the priority document to the International Bureau. Such request must be made before the expiration of the 16-month time limit and may be subjected by the receiving Office to the payment of a fee (Rule 17.1(b)).

If the priority document concerned is not submitted to the International Bureau or if the request to the receiving Office to prepare and transmit the priority document has not been made (and the corresponding fee, if any, paid) within the applicable time limit indicated under the preceding paragraphs, any designated State may disregard the priority claim, provided that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity to furnish the priority document within a time limit which is reasonable under the circumstances.

Where several priorities are claimed, the priority date to be considered for the purposes of computing the 16-month time limit is the filing date of the earliest application whose priority is claimed.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Translation

Applicant's or agent's file reference FH990804PCT	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP99/06312	International filing date (<i>day/month/year</i>) 27 August 1999 (27.08.99)	Priority date (<i>day/month/year</i>) 22 September 1998 (22.09.98)
International Patent Classification (IPC) or national classification and IPC G07F 7/10		
Applicant FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.		

<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>6</u> sheets, including this cover sheet.</p> <p><input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of <u>10</u> sheets.</p>
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input type="checkbox"/> Certain defects in the international application</p> <p>VIII <input type="checkbox"/> Certain observations on the international application</p>

Date of submission of the demand 06 April 2000 (06.04.00)	Date of completion of this report 22 September 2000 (22.09.2000)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP99/06312

I. Basis of the report

1. This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.):

☒ the international application as originally filed.

☒ the description, pages 1,2,4-20, as originally filed,
pages _____, filed with the demand,
pages 3,3a-3b, filed with the letter of 02 August 2000 (02.08.2000),
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-18, filed with the letter of 02 August 2000 (02.08.2000),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/4-4/4, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP 99/06312

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability: citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-18	YES
	Claims		NO
Inventive step (IS)	Claims	1-18	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following documents:

D1: EP-A-0 313 967 (GAO GES AUTOMATION ORG) 3 May 1989 (1989-05-03)

D2: EP-A-0 654 919 (SIEMENS AG) 24 May 1995 (1995-05-24)

D3: W. RANKL & W. EFFING: 'Handbuch der Chipkarten' 10 February 1998 (1998-02-10), CARL HANSER VERLAG, MÜNCHEN WIEN XP002127583 022759.

The essential difference between the concept of D1 and the concept of the invention consists in the fact that, according to D1 the individual characterising data in the memory (53) is always the same, irrespective of the random number stored in the card (51). In the invention, however, it is essential that the operational data of the circuit also depends on the input data of the circuit. Document D1 does not disclose a device for determining the operational data of the electronic circuit, said data being influenced by an operation of the electronic circuit, when the electronic circuit executes the algorithm. Moreover, in D1 the individual stored data is not dependent on the input

data, that is the random number, which is transmitted from block Z in Figure 11 to block RN. Consequently, document D1 also fails to disclose a device for determining the operational data of the electronic circuit (the operational data of the device (60) in Figure 11 is not determined; the memory (52) is not an element that generates output data from the card depending on input data in the card). Furthermore, D1 does not disclose the fact that the algorithm, which is executed by the electronic circuit, uses the determined operational data of the electronic circuit, since such operational data of the electronic circuit is not even determined.

Proceeding from D1, the invention addresses the problem of developing a concept for the improved protection of electronic circuits and therefore of developing a secure method for authenticating such electronic circuits and a secure method for authorising an owner of such electronic circuits.

This problem is solved as per the invention by a device according to Claim 1 and a method according to Claims 17 or 18.

The solution defined in the independent claims involves an inventive step: unlike in D1, the invention does not use the individual characterising data of just any electronic circuit, but rather the operational data of the electronic circuit which generates output data depending on the input data. The concept as per the invention dispenses with the storing of characterising data in a central processor.

The teaching of D1 differs from the solution as per the invention in that in D1 the individual characterising data in the memory is always the same and can therefore be stored at the beginning, whereas according to the invention, the operational data depends on the input data and therefore a single storage of the operational data would not make any sense. D2 and D3 point further away from the subject matter of the present invention than D1. Although these documents specify different authentication procedures between a transmitter and a receiver, they do not suggest using the technological operational patterns of output data from a card that is to be authorised.

There are no objections concerning industrial applicability.

Consequently, independent Claims 1, 17 and 18 would appear to meet the criteria for novelty, inventive step and industrial applicability stipulated in PCT Article 33(1). Claims 2-16 concern advantageous configurations and therefore also satisfy said criteria.

It is the applicant's opinion that delimitation over D1 would lead to a claim that would be difficult to understand and therefore the one-part form has been used for Claim 1. Since it is sufficiently clear from the detailed discussion of D1 in the description which features of Claim 1 are already known from the prior art, in line with the PCT Guidelines PCT/GL/3, Chapter III-2.3a, the use of the two-part form under PCT Rule 5.1(a)(ii) is not required in this case.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: INTERNATIONALE RECHERCHENBEHÖRDE

An
SCHOPPE, ZIMMERMANN & STÖCKELER
z.H. Schoppe, Fritz
Postfach 71 08 67
D-81458 München
GERMANY

31 JAN. 2000

MITTEILUNG ÜBER
INTERNATIONALE
ODER DE

International

Search

Report &

Prior Art References

(Regel 44.1 PCT)

Absenddatum
(Tag/Monat/Jahr)

28/01/2000

Aktenzeichen des Anmelders oder Anwalts

FH990804PCT

WEITERES VORGEHEN

siehe Punkte 1 und 4 unten

Internationales Aktenzeichen

PCT/EP 99/ 06312

Internationales Anmeldedatum

(Tag/Monat/Jahr)

27/08/1999

Anmelder

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG... ET AL.

1. ☒ Dem Anmelder wird mitgeteilt, daß der Internationale Recherchenbericht erstellt wurde und ihm hiermit übermittelt wird.
Einreichung von Änderungen und einer Erklärung nach Artikel 19:
Der Anmelder kann auf eigenen Wunsch die Ansprüche der internationalen Anmeldung ändern (siehe Regel 46):

Bis wann sind Änderungen einzureichen?

Die Frist zur Einreichung solcher Änderungen beträgt üblicherweise zwei Monate ab der Übermittlung des internationalen Recherchenberichts; weitere Einzelheiten sind den Anmerkungen auf dem Beiblatt zu entnehmen.

Wo sind Änderungen einzureichen?

Unmittelbar beim Internationalen Büro der WIPO, 34, CHEMIN des Colombettes, CH-1211 Genf 20,
Telefaxnr.: (41-22) 740.14.35

Nähere Hinweise sind den Anmerkungen auf dem Beiblatt zu entnehmen.

2. ☐ Dem Anmelder wird mitgeteilt, daß kein internationaler Recherchenbericht erstellt wird und daß ihm hiermit die Erklärung nach Artikel 17(2)a) übermittelt wird.
3. ☐ Hinsichtlich des Widerspruchs gegen die Entrichtung einer zusätzlichen Gebühr (zusätzlicher Gebühren) nach Regel 40.2 wird dem Anmelder mitgeteilt, daß
- ☐ der Widerspruch und die Entscheidung hierüber zusammen mit seinem Antrag auf Übermittlung des Wortlauts sowohl des Widerspruchs als auch der Entscheidung hierüber an die Bestimmungsämter dem Internationalen Büro übermittelt worden sind.
- ☐ noch keine Entscheidung über den Widerspruch vorliegt; der Anmelder wird benachrichtigt, sobald eine Entscheidung getroffen wurde.

4. Weiteres Vorgehen: Der Anmelder wird auf folgendes aufmerksam gemacht:

Kurz nach Ablauf von 18 Monaten seit dem Prioritätsdatum wird die internationale Anmeldung vom Internationalen Büro veröffentlicht. Will der Anmelder die Veröffentlichung verhindern oder auf einen späteren Zeitpunkt verschieben, so muß gemäß Regel 90^{bis} bzw. 90^{ter} vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung eine Erklärung über die Zurücknahme der internationalen Anmeldung oder des Prioritätsanspruchs beim Internationalen Büro eingehen.

Innerhalb von 19 Monaten seit dem Prioritätsdatum ist ein Antrag auf internationale vorläufige Prüfung einzureichen, wenn der Anmelder den Eintritt in die nationale Phase bis zu 30 Monaten seit dem Prioritätsdatum (in manchen Ämtern sogar noch länger) verschieben möchte.

Innerhalb von 20 Monaten seit dem Prioritätsdatum muß der Anmelder die für den Eintritt in die nationale Phase vorgeschriebenen Handlungen vor allen Bestimmungsämtern vornehmen, die nicht innerhalb von 19 Monaten seit dem Prioritätsdatum in der Anmeldung oder einer nachträglichen Auswahlklärung ausgewählt wurden oder nicht ausgewählt werden konnten, da für sie Kapitel II des Vertrages nicht verbindlich ist.

Name und Postanschrift der Internationalen Recherchenbehörde



Europäisches Patentamt, P.B. 5818 Patentaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Bevollmächtigter Bediensteter

Louis Ka inde

Diese Anmerkungen sollen grundlegende Hinweise zur Einreichung von Änderungen gemäß Artikel 19 geben. Diesen Anmerkungen liegen die Erfordernisse des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (PCT), der Ausführungsordnung und der Verwaltungsrichtlinien zu diesem Vertrag zugrunde. Bei Abweichungen zwischen diesen Anmerkungen und obengenannten Texten sind letztere maßgebend. Nähere Einzelheiten sind dem PCT-Leitfaden für Anmelder, einer Veröffentlichung der WIPO, zu entnehmen.

Die in diesen Anmerkungen verwendeten Begriffe "Artikel", "Regel" und "Abschnitt" beziehen sich jeweils auf die Bestimmungen des PCT-Vertrags, der PCT-Ausführungsordnung bzw. der PCT-Verwaltungsrichtlinien.

HINWEISE ZU ÄNDERUNGEN GEMÄSS ARTIKEL 19

Nach Erhalt des internationalen Recherchenberichts hat der Anmelder die Möglichkeit, einmal die Ansprüche der internationalen Anmeldung zu ändern. Es ist jedoch zu betonen, daß, da alle Teile der internationalen Anmeldung (Ansprüche, Beschreibung und Zeichnungen) während des internationalen vorläufigen Prüfungsverfahrens geändert werden können, normalerweise keine Notwendigkeit besteht, Änderungen der Ansprüche nach Artikel 19 einzureichen, außer wenn der Anmelder z.B. zum Zwecke eines vorläufigen Schutzes die Veröffentlichung dieser Ansprüche wünscht oder ein anderer Grund für eine Änderung der Ansprüche vor ihrer internationalen Veröffentlichung vorliegt. Weiterhin ist zu beachten, daß ein vorläufiger Schutz nur in einigen Staaten erhältlich ist.

Welche Teile der internationalen Anmeldung können geändert werden?

Im Rahmen von Artikel 19 können nur die Ansprüche geändert werden.

In der internationalen Phase können die Ansprüche auch nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert (oder nochmals geändert) werden. Die Beschreibung und die Zeichnungen können nur nach Artikel 34 vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde geändert werden.

Beim Eintritt in die nationale Phase können alle Teile der internationalen Anmeldung nach Artikel 28 oder gegebenenfalls Artikel 41 geändert werden.

Bis wann sind Änderungen einzureichen?

Innerhalb von zwei Monaten ab der Übermittlung des internationalen Recherchenberichts oder innerhalb von sechzehn Monaten ab dem Prioritätsdatum, je nachdem, welche Frist später abläuft. Die Änderungen gelten jedoch als rechtzeitig eingereicht, wenn sie dem internationalen Büro nach Ablauf der maßgebenden Frist, aber noch vor Abschluß der technischen Vorbereitungen für die internationale Veröffentlichung (Regel 46.1) zugehen.

Wo sind die Änderungen nicht einzureichen?

Die Änderungen können nur beim Internationalen Büro, nicht aber beim Anmeldeamt oder der Internationalen Recherchenbehörde eingereicht werden (Regel 46.2).

Falls ein Antrag auf internationale vorläufige Prüfung eingereicht wurde/wird, siehe unten.

In welcher Form können Änderungen erfolgen?

Eine Änderung kann erfolgen durch Streichung eines oder mehrerer ganzer Ansprüche, durch Hinzufügung eines oder mehrerer neuer Ansprüche oder durch Änderung des Wortlauts eines oder mehrerer Ansprüche in der eingereichten Fassung.

Für jedes Anspruchsblatt, das sich aufgrund einer oder mehrerer Änderungen von dem ursprünglich eingereichten Blatt unterscheidet, ist ein Ersatzblatt einzureichen.

Alle Ansprüche, die auf einem Ersatzblatt erscheinen, sind mit arabischen Ziffern zu numerieren. Wird ein Anspruch gestrichen, so brauchen, die anderen Ansprüche nicht neu numeriert zu werden. Im Fall einer Neunummerierung sind die Ansprüche fortlaufend zu numerieren (Verwaltungsrichtlinien, Abschnitt 205 b)).

Die Änderungen sind in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Welche Unterlagen sind den Änderungen beizufügen?

Begleitschreiben (Abschnitt 205 b)):

Die Änderungen sind mit einem Begleitschreiben einzureichen.

Das Begleitschreiben wird nicht zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht. Es ist nicht zu verwechseln mit der "Erklärung nach Artikel 19(1)" (siehe unten, "Erklärung nach Artikel 19 (1)").

Das Begleitschreiben ist nach Wahl des Anmelders in englischer oder französischer Sprache abzufassen. Bei englischsprachigen internationalen Anmeldungen ist das Begleitschreiben aber ebenfalls in englischer, bei französischsprachigen internationalen Anmeldungen in französischer Sprache abzufassen.

ANMERKUNGEN ZU FORMBLATT PCT/ISA/220 (Fortsetzung)

Im Begleitschreiben sind die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen anzugeben. So ist insbesondere zu jedem Anspruch in der internationalen Anmeldung anzugeben (gleichlautende Angaben zu verschiedenen Ansprüchen können zusammengefaßt werden), ob

- i) der Anspruch unverändert ist;
- ii) der Anspruch gestrichen worden ist;
- iii) der Anspruch neu ist;
- iv) der Anspruch einen oder mehrere Ansprüche in der eingereichten Fassung ersetzt;
- v) der Anspruch auf die Teilung eines Anspruchs in der eingereichten Fassung zurückzuführen ist.

Im folgenden sind Beispiele angegeben, wie Änderungen im Begleitschreiben zu erläutern sind:

1. [Wenn anstelle von ursprünglich 48 Ansprüchen nach der Änderung einiger Ansprüche 51 Ansprüche existieren]:
"Die Ansprüche 1 bis 29, 31, 32, 34, 35, 37 bis 48 werden durch geänderte Ansprüche gleicher Numerierung ersetzt; Ansprüche 30, 33 und 36 unverändert; neue Ansprüche 49 bis 51 hinzugefügt."
2. [Wenn anstelle von ursprünglich 15 Ansprüchen nach der Änderung aller Ansprüche 11 Ansprüche existieren]:
"Geänderte Ansprüche 1 bis 11 treten an die Stelle der Ansprüche 1 bis 15."
3. [Wenn ursprünglich 14 Ansprüche existierten und die Änderungen darin bestehen, daß einige Ansprüche gestrichen werden und neue Ansprüche hinzugefügt werden]:
Ansprüche 1 bis 6 und 14 unverändert; Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt. "Oder" Ansprüche 7 bis 13 gestrichen; neue Ansprüche 15, 16 und 17 hinzugefügt; alle übrigen Ansprüche unverändert."
4. [Wenn verschiedene Arten von Änderungen durchgeführt werden]:
"Ansprüche 1-10 unverändert; Ansprüche 11 bis 13, 18 und 19 gestrichen; Ansprüche 14, 15 und 16 durch geänderten Anspruch 14 ersetzt; Anspruch 17 in geänderte Ansprüche 15, 16 und 17 unterteilt; neue Ansprüche 20 und 21 hinzugefügt."

"Erklärung nach Artikel 19(1)" (Regel 46.4)

Den Änderungen kann eine Erklärung beigefügt werden, mit der die Änderungen erläutert und ihre Auswirkungen auf die Beschreibung und die Zeichnungen dargelegt werden (die nicht nach Artikel 19 (1) geändert werden können).

Die Erklärung wird zusammen mit der internationalen Anmeldung und den geänderten Ansprüchen veröffentlicht.

Sie ist in der Sprache abzufassen, in der die internationale Anmeldung veröffentlicht wird.

Sie muß kurz gehalten sein und darf, wenn in englischer Sprache abgefaßt oder ins Englische übersetzt, nicht mehr als 500 Wörter umfassen.

Die Erklärung ist nicht zu verwechseln mit dem Begleitschreiben, das auf die Unterschiede zwischen den Ansprüchen in der eingereichten Fassung und den geänderten Ansprüchen hinweist, und ersetzt letzteres nicht. Sie ist auf einem gesonderten Blatt einzureichen und in der Überschrift als solche zu kennzeichnen, vorzugsweise mit den Worten "Erklärung nach Artikel 19 (1)".

Die Erklärung darf keine herabsetzenden Äußerungen über den internationalen Recherchenbericht oder die Bedeutung von in dem Bericht angeführten Veröffentlichungen enthalten. Sie darf auf im internationalen Recherchenbericht angeführte Veröffentlichungen, die sich auf einen bestimmten Anspruch beziehen, nur im Zusammenhang mit einer Änderung dieses Anspruchs Bezug nehmen.

Auswirkungen eines bereits gestellten Antrags auf internationale vorläufige Prüfung

Ist zum Zeitpunkt der Einreichung von Änderungen nach Artikel 19 bereits ein Antrag auf internationale vorläufige Prüfung gestellt worden, so sollte der Anmelder in seinem Interesse gleichzeitig mit der Einreichung der Änderungen beim Internationalen Büro auch eine Kopie der Änderungen bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde einreichen (siehe Regel 62.2 a), erster Satz).

Auswirkungen von Änderungen hinsichtlich der Übersetzung der internationalen Anmeldung beim Eintritt in die nationale Phase

Der Anmelder wird darauf hingewiesen, daß bei Eintritt in die nationale Phase möglicherweise anstatt oder zusätzlich zu der Übersetzung der Ansprüche in der eingereichten Fassung eine Übersetzung der nach Artikel 19 geänderten Ansprüche an die bestimmten/ausgewählten Ämter zu übermitteln ist.

Nähere Einzelheiten über die Erfordernisse jedes bestimmten/ausgewählten Amtes sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts FH990804PCT	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/EP 99/06312	Internationales Anmeldedatum (Tag/Monat/Jahr) 27/08/1999	(Früheste) Prioritätsdatum (Tag/Monat/Jahr) 22/09/1998
Anmelder FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG... ET AL.		

Dieser Internationale Recherchenbericht wurde von der internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem internationalen Büro übermittelt.

Dieser Internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

a. Hinsichtlich der Sprache ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

b. Hinsichtlich der in der internationalen Anmeldung offenbarten Nucleotid- und/oder Aminosäuresequenz ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der Zusammenfassung

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

☒ wie vom Anmelder vorgeschlagen

☐ keine der Abb.

☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

A. KLASSIFIZIERUNG DES VERMELDUNGSGEGENSTANDES
IPK 7 G07F7/00

Nach der internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G07F G09C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 313 967 A (GAO GES AUTOMATION ORG) 3. Mai 1989 (1989-05-03)	1,3-5,7, 10-12
Y	Spalte 1, Absatz 3 Spalte 5, Zeile 54 - Spalte 6, Zeile 3 Spalte 6, Zeile 49 - Spalte 7, Zeile 5 Spalte 7, Zeile 29 - Zeile 33 Spalte 8, Zeile 17 - Zeile 26	17,18
A		2,6,13, 16
Y	W. RANKL & W. EFFING: "Handbuch der Chipkarten" 10. Februar 1998 (1998-02-10), CARL HANSER VERLAG, MÜNCHEN WIEN XP002127583 022759	17
A	Seite 276 -Seite 277 Abbildung 8.13	1,4,5

-/-

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"I" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

14. Januar 2000

Abmeldedatum des internationalen Recherchenberichts

28/01/2000

Name und Postanschrift der internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Bevollmächtigter Bediensteter

Wolles, B

C.(Fortsetzung) ALS WICHTIGSTES ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP 0 654 919 A (SIEMENS AG) 24. Mai 1995 (1995-05-24) Zusammenfassung	18

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 99/06312

Im Recherchen angeführtes Patentdokument	Datum der Veröffentlichung	Mitglieder der Patentfamilie	Datum der Veröffentlichung
EP 0313967 A	03-05-1989	DE 3736882 A AT 87383 T DE 3879616 A WO 8904022 A HK 60395 A JP 2501961 T JP 2925152 B US 5818738 A	13-07-1989 15-04-1993 29-04-1993 05-05-1989 28-04-1995 28-06-1990 28-07-1999 06-10-1998
EP 0654919 A	24-05-1995	DE 4339460 C	06-04-1995

PCT-ANTRAG

1/4

Original (für EINREICHUNG) - gedruckt am 27.08.1999 0

International
Patent Application
as originally
filed

PCT

0	Vom Anmeldeamt auszufüllen	
0-1	Internationales Aktenzeichen.	
0-2	Internationales Anmeldedatum	
0-3	Name des Anmeldeamts und "PCT International Application"	
0-4	Formular - PCT/RO/101 PCT-Antrag	
0-4-1	erstellt durch Benutzung von	PCT-EASY Version 2.84 (aktualisiert 01.07.1999)
0-5	Antragsersuchen Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird	
0-6	(Vom Anmelder gewähltes) Anmeldeamt	Europäisches Patentamt (EPA) (RO/EP)
0-7	Aktenzeichen des Anmelders oder Anwalts	FH990804PCT
I	Bezeichnung der Erfindung	VORRICHTUNG ZUM LIEFERN VON AUSGANGSDATEN ALS REAKTION AUF EINGANGSDATEN UND VERFAHREN ZUM ÜBERPRÜFEN DER AUTHENTIZITÄT UND VERFAHREN ZUM VERSCHLÜSSELTEN ÜBERTRAGEN VON INFORMATIONEN
II	Anmelder	
II-1	Diese Person ist	nur Anmelder
II-2	Anmelder für	Alle Bestimmungstaaten mit Ausnahme von US
II-4	Name	FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
II-5	Anschrift:	Leonrodstraße 54 D-80636 München Deutschland
II-6	Staatsangehörigkeit (Staat)	DE
II-7	Sitz/Wohnsitz (Staat)	DE
III-1	Anmelder und/oder Erfinder	
III-1-1	Diese Person ist	Anmelder und Erfinder
III-1-2	Anmelder für	Nur US
III-1-4	Name (FAMILIENNAME, Vorname)	OELMAIER, Florian
III-1-5	Anschrift:	Gründlacher Straße 15 D-91058 Erlangen Deutschland
III-1-6	Staatsangehörigkeit (Staat)	DE
III-1-7	Sitz/Wohnsitz (Staat)	DE

PCT-ANTRAG

FH990804PCT

Original (für EINREICHUNG) - gedruckt am 27.08.1999 01:07:41 PM

III-2	Anmelder und/oder Erfinder	
III-2-1	Diese Person ist	Anmelder und Erfinder
III-2-2	Anmelder für	Nur US
III-2-4	Name (FAMILIENNAME, Vorname)	BRAND, Roland
III-2-5	Anschrift:	Pfinzingweg 13 D-91058 Erlangen Deutschland
III-2-6	Staatsangehörigkeit (Staat)	DE
III-2-7	Sitz/Wohnsitz (Staat)	DE
III-3	Anmelder und/oder Erfinder	
III-3-1	Diese Person ist	Anmelder und Erfinder
III-3-2	Anmelder für	Nur US
III-3-4	Name (FAMILIENNAME, Vorname)	HEUER, André
III-3-5	Anschrift:	Stintzingstraße 29 D-91052 Erlangen Deutschland
III-3-6	Staatsangehörigkeit (Staat)	DE
III-3-7	Sitz/Wohnsitz (Staat)	DE
III-4	Anmelder und/oder Erfinder	
III-4-1	Diese Person ist	Anmelder und Erfinder
III-4-2	Anmelder für	Nur US
III-4-4	Name (FAMILIENNAME, Vorname)	GERHÄUSER, Heinz
III-4-5	Anschrift:	Saugendorf 17 D-91344 Waischenfeld Deutschland
III-4-6	Staatsangehörigkeit (Staat)	DE
III-4-7	Sitz/Wohnsitz (Staat)	DE
III-5	Anmelder und/oder Erfinder	
III-5-1	Diese Person ist	Anmelder und Erfinder
III-5-2	Anmelder für	Nur US
III-5-4	Name (FAMILIENNAME, Vorname)	PROSCH, Markus
III-5-5	Anschrift:	Fürther Straße 31 D-91058 Erlangen Deutschland
III-5-6	Staatsangehörigkeit (Staat)	DE
III-5-7	Sitz/Wohnsitz (Staat)	DE
III-6	Anmelder und/oder Erfinder	
III-6-1	Diese Person ist	Anmelder und Erfinder
III-6-2	Anmelder für	Nur US
III-6-4	Name (FAMILIENNAME, Vorname)	KORTE, Olaf
III-6-5	Anschrift:	Etlaswind 19 D-91338 Igendorf Deutschland
III-6-6	Staatsangehörigkeit (Staat)	DE
III-6-7	Sitz/Wohnsitz (Staat)	DE

III-7	Anmelder und/oder Erfinder	
III-7-1	Diese Person ist	Anmelder und Erfinder
III-7-2	Anmelder für	Nur US
III-7-4	Name (FAMILIENNAME, Vorname)	PLANKENBÜHLER, Roland
III-7-5	Anschrift:	Grazer Straße 7 D-90475 Nürnberg Deutschland
III-7-6	Staatsangehörigkeit (Staat)	DE
III-7-7	Sitz/Wohnsitz (Staat)	DE
IV-1	Anwalt oder gemeinsamer Vertreter; oder besondere Zustellanschrift Die unten bezeichnete Person ist/wird hiermit bestellt, um den (die) Anmelder vor den internationalen Behörden zu vertreten, und zwar als:	Anwalt
IV-1-1	Name (FAMILIENNAME, Vorname)	SCHOPPE, Fritz
IV-1-2	Anschrift:	SCHOPPE, ZIMMERMANN & STÖCKELER POSTFACH 71 08 67 D-81458 München Deutschland
IV-1-3	Telefonnr.	089/7904450
IV-1-4	Telefaxnr.	089/7902215
IV-1-5	e-mail	101345.3117@CompuServe.com
V	Bestimmung von Staaten	
V-1	Regionales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE und jeder weitere Staat, der Mitgliedsstaat des Europäischen Patentübereinkommens und Vertragsstaat des PCT ist
V-2	Nationales Patent (andere Schutzrechtsarten oder Verfahren sind ggf. in Klammern nach der (den) betreffenden Bestimmung(en) angegeben)	CA US
V-5	Erklärung bzgl. vorsorglicher Bestimmungen Zusätzlich zu den unter Punkten V-1, V-2 and V-3 vorgenommenen Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der nachstehend unter Punkt V-6 angegebenen Staaten. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt.	
V-6	Staaten, die von der Erklärung über vorsorgliche Bestimmungen ausgenommen werden	KEINE

PCT-ANTRAG

FH990804PCT

Original (für EINREICHUNG) - gedruckt am 27.08.1999 01:07:41 PM

VI-1	Priorität einer früheren nationalen Anmeldung beansprucht		
VI-1-1	Anmeldedatum	22 September 1998 (22.09.1998)	
VI-1-2	Aktenzeichen	19843424.3	
VI-1-3	Staat	DE	
VII-1	Gewählte Internationale Recherchenbehörde	Europäisches Patentamt (EPA) (ISA/EP)	
VIII	Kontrollliste	Anzahl der Blätter	Elektronische Datei(en) beigefügt
VIII-1	Antrag	4	-
VIII-2	Beschreibung	20	-
VIII-3	Ansprüche	5	-
VIII-4	Zusammenfassung	1	fh990804.txt
VIII-5	Zeichnung(en)	4	-
VIII-7	INSGESAMT	34	
VIII-8	Beigefügte Unterlagen	Unterlage(n) in Papierform beigefügt	Elektronische Datei(en) beigefügt
VIII-10	Blatt für die Gebührenberechnung	✓	-
VIII-16	Kopie der allgemeinen Vollmacht	Aktenzeichen 17406	-
VIII-18	PCT-EASY-Diskette	-	Diskette
VIII-19	Nr. der Abb. der Zeichn., die mit der Zusammenf. veröffentlicht werden soll	1	
IX-1	Sprache der int. Anmeldung	Deutsch	
IX-1-1	Unterschrift des Anmelders oder Anwalts		
IX-1-1	Name (FAMILIENNAME, Vorname)	SCHOPPE, Fritz	

VOM ANMELDEAMT AUSZUFÜLLEN

10-1	Datum des tatsächlichen Eingangs dieser Internationalen Anmeldung	
10-2	Zeichnung(en):	
10-2-1	Eingegangen	
10-2-2	Nicht eingegangen	
10-3	Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingeg. Unterlage(n) oder Zeichnung(en) zur Vervollständigung dieser int. Anmeldung	
10-4	Datum des fristgerechten Eingangs der Berichtigung nach PCT Artikel 11(2)	
10-5	Internationale Recherchenbehörde	ISA/EP
10-6	Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchegebühr aufgeschoben	

VOM INTERNATIONALEN BÜRO AUSZUFÜLLEN

11-1	Datum des Eingangs des Aktenexemplars beim Internationalen Büro	
------	---	--

Patentanwälte · Postfach 710867 · 81458 München

Fraunhofer-Gesellschaft
zur Förderung der
angewandten Forschung e. V.
Leonrodstraße 54
D-80636 München
DE

PATENTANWÄLTE

European Patent Attorneys
European Trademark Attorneys

Fritz Schoppe, Dipl.-Ing.
Tankred Zimmermann, Dipl.-Ing.
Ferdinand Stöckeler, Dipl.-Ing.

Telefon/Telephone 089/790445-0
Telefax/Facsimile 089/790 22 15
Telefax/Facsimile 089/74996977
e-mail 101345.3117@CompuServe.com

**Vorrichtung zum Liefern von Ausgangsdaten als Reaktion auf
Eingangsdaten und Verfahren zum Überprüfen der Authentizität
und Verfahren zum verschlüsselten Übertragen von Informationen**

VORRICHTUNG ZUM LIEFERN VON AUSGANGSDATEN ALS REAKTION AUF
EINGANGSDATEN UND VERFAHREN ZUM ÜBERPRÜFEN DER AUTHENTIZITÄT
UND VERFAHREN ZUM VERSCHLÜSSELTEN ÜBERTRAGEN VON
INFORMATIONEN

Beschreibung

Die vorliegende Erfindung bezieht sich auf die Überprüfung der Authentizität in manipulierversicherten Systemen und insbesondere auf eine Vorrichtung zum Liefern von Ausgangsdaten als Reaktion auf Eingangsdaten, um abhängig von den Ausgangsdaten die Authentizität der Vorrichtung zu bestimmen, und auf Verfahren, die solche Vorrichtungen verwenden.

Heutzutage werden oft integrierte Schaltungen verwendet, die auf einer Chipkarte aufgebracht bzw. in einer Chipkarte eingebracht sind, um den Inhaber der integrierten Schaltungen bezüglich seiner Autorisierung zu überprüfen, eine bestimmte Handlung vorzunehmen, wobei zur Sicherung gegen gefälschte Karten zusätzlich eine Überprüfung der Authentizität der integrierten Schaltungen durchgeführt wird. Solche integrierten Schaltungen werden in Form von Smart Cards, wie sie in den Standard ISO 7816 definiert sind, oder in der Form von PC-Cards, wie sie in PCMCIA's PC CARD Standard, Ausgabe 6.1 definiert sind, eingesetzt. Weitere Anwendungsgebiete neben den genannten Möglichkeiten bestehen überall dort, wo Chipkarten verwendet werden, beispielsweise in Form von Telefonkarten oder Karten, die einen Zugang zu bestimmten Gebäuden ermöglichen, d. h. die als elektronische Schlüssel fungieren.

Wesentlich an den integrierten Schaltungen, die in solchen Karten zu finden sind, ist, daß nur der Benutzer, der im Besitz einer solchen Karte ist, auch den Zugang erhält oder z. B. ein verschlüsseltes Fernsehprogramm mittels seiner Smart Card entschlüsseln kann. Die Autorisierung erfolgt

dabei z. B. durch Bezahlen, wenn an Telefonkarten oder Smart Cards in Verbindung mit Pay-TV gedacht wird, oder durch Erlauben einer bestimmten Funktion, wenn elektronische Schlüsselsel verwendet werden.

Um sicherzustellen, daß nur berechnigte Personen, d. h. Personen, die beispielsweise eine Telefonkarte erworben haben, telefonieren, ist es entscheidend, gefälschte Karten zu erkennen und Inhabern von gefälschten Karten am Beispiel von Telefonkarten das Telefonieren zu verbieten. Obwohl kein hundertprozentiger Schutz gegen Nachahmer existiert, besteht doch die Möglichkeit, Fälschern von Karten, die die Funktion der Karten nachahmen, so viel Schwierigkeiten als möglich zu bereiten.

Fälscher haben viel Einfallsreichtum aufgewendet, um die Funktionalität einer Chipkarte bzw. einer integrierten Schaltung zu kopieren. Eine Möglichkeit besteht beispielsweise darin, den Chip einer Chipkarte abzuschleifen und anhand des Layouts der integrierten Schaltung auf die Funktionalität des auf der Karte implementierten Algorithmus zu schließen. Dann kann die Funktionalität der Karte, d. h. der Algorithmus, der aufgrund eines Eingangswertes in die Karte einen Ausgangswert erzeugt, der von einem Kartenleser ausgewertet wird, mittels eines Computers simuliert werden. Hat ein Fälscher das Layout z. B. einer Telefonkarte ermittelt, so könnte er eine Simulationskarte, die mit einem Computer verbunden ist, in den Kartenleseschlitz eines Kartentelefons einführen und das Verhalten der Karte bei der Authentizitätsprüfung simulieren.

Selbstverständlich existieren gegenüber solchen Angriffen auch mechanische Schutzmechanismen, die beispielsweise, wenn die Karte in ein Lesegerät eingeführt ist, einen Zugriff von außen auf die Karte unterbinden. Wie es jedoch in der Fachveröffentlichung "Tamper Resistance A Cautionary Note; Proceedings - The Second USENIX Workshop on Electronic

Commerce, von Markus Kuhn und Ross Anderson, dargestellt worden ist, existieren viele Fälschungsverfahren, die weiterhin den anhaltenden Bedarf nach besseren Schutzmechanismen für Schaltungen und insbesondere für integrierte Schaltungen auf einer Chipkarte unterstreichen. Übliche Datenverschlüsselungsverfahren, die beispielsweise auf dem DES-Algorithmus basieren (DES Data Encryption Standard) oder die Prüfsummenalgorithmen umfassen, liefern zwar eine hohe Sicherheit, wenn der Verschlüsselungsschlüssel, der zusammen mit dem Krypto-Algorithmus eine Entschlüsselung ermöglicht, geheimgehalten wird. Prinzipiell ist es jedoch auch hier möglich, einen solchen Algorithmus, der in Form einer integrierten Schaltung auf einer Chipkarte hardware-mäßig integriert ist, anhand der Hardware-Implementation nachzuahmen, d. h. dessen Funktionalität beispielsweise mittels eines Computers zu simulieren.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Konzept zum verbesserten Schutz von elektronischen Schaltungen zu schaffen und somit eine fälschungssicherere Überprüfung der Authentizität solcher elektronischen Schaltungen und eine fälschungssicherere Autorisierung eines Inhabers solcher elektronischer Schaltungen zu schaffen.

Diese Aufgabe wird durch eine Vorrichtung nach Anspruch 1 und durch ein Verfahren nach Anspruch 17 oder 18 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß es zwar relativ einfach ist die Funktionalität eines Chips zu kopieren, daß es jedoch viel schwieriger ist, dessen Zeit- oder Leistungsverhalten nachzubilden. Eine Vorrichtung zum Liefern von Ausgangsdaten als Reaktion auf Eingangsdaten, um abhängig von den Ausgangsdaten die Authentizität der Vorrichtung zu bestimmen, umfaßt daher einerseits eine elektronische Schaltung zum Ausführen eines Algorithmus, der aus den Eingangsdaten die Ausgangsdaten erzeugt, und andererseits eine Einrichtung zum Erfassen von

Betriebsdaten, die durch einen Betrieb der elektronischen Schaltung beeinflußt werden, wobei die Einrichtung zum Erfassen von Daten mit der elektronischen Schaltung derart gekoppelt ist, daß die Betriebsdaten der elektronischen Schaltung durch den Algorithmus verwendet werden, um die Ausgangsdaten zu erzeugen.

Bei einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung implementiert die elektronische Schaltung einen kryptographischen Algorithmus, der die Einrichtung zum Erfassen von Betriebsdaten aufruft, um Zeit- und/oder Leistungsmessungen durchzuführen, die neben den Eingangsdaten durch die elektronische Schaltung verwendet werden, um die Ausgangsdaten zu erzeugen. Die Ausgangsdaten stellen daher eine Kombination der Funktionalität des kryptographischen Algorithmus und der Betriebsdaten, die die Schaltung zum Ausführen des kryptographischen Algorithmus aufweist, dar. Ein Angriff auf die erfindungsgemäße Vorrichtung muß also nicht nur den kryptographischen Algorithmus sondern auch den Leistungsverbrauch und/oder das zeitliche Verhalten der elektronischen Schaltung während der Ausführung des kryptographischen Algorithmus nachbilden.

Eine Vielzahl von kryptographischen Algorithmen ist in dem Fachbuch "Applied Cryptography" von Bruce Schneier dargestellt.

Betriebsdaten der integrierten Schaltung, die beim Erzeugen der Ausgangsdaten verwendet werden, sind vorzugsweise der Leistungsverbrauch und die Laufzeit des Algorithmus in der elektronischen Schaltung. Solche Betriebs- oder "Umgebungs"-Daten können jedoch alle Daten sein, die durch einen Betrieb der elektronischen Schaltung beeinflußt werden, wie z. B. eine von der elektronischen Schaltung abgegebene elektromagnetische Strahlung und dergleichen. Grenzen für die Verwendung von Betriebsdaten bestehen darin, wie dieselben in einer praktischen Ausführung gemessen werden

können, wenn zum Beispiel an elektromagnetische Strahlung gedacht wird. Bevorzugt werden daher aufgrund der leichten Meßbarkeit, Leistungsdaten und Daten bezüglich des zeitlichen Verhaltens der elektronischen Schaltung als Betriebsdaten verwendet.

Grundsätzlich ist es nicht erforderlich, daß der Algorithmus ein kryptographischer Algorithmus ist. Derselbe könnte irgendein Algorithmus sein, der abhängig von unterschiedlichen Eingangsdaten unterschiedliche Betriebsdaten aufweist. Der Schutz gegen eine Fälschung ist jedoch umso besser, je "chaotischer" die Abhängigkeit der Betriebsdaten von unterschiedlichen Eingangsdaten ist.

Zur Verbesserung des Schutzes wird es bevorzugt, als Algorithmus einen Krypto-Algorithmus einzusetzen, der an sich einen Schutz gegen Fälschung liefert, der durch die erfindungsgemäße Berücksichtigung der Betriebsdaten der elektronischen Schaltung, die diesen kryptographischen Algorithmus ausführt, erhöht wird. Üblicherweise werden Algorithmen jedoch dahingehend entworfen, daß sie ein relativ konstantes Laufzeitverhalten unabhängig von den Eingabewerten aufweisen. Um die Sicherheit weiter zu erhöhen, wird der Algorithmus, der durch die elektronische Schaltung ausgeführt wird, bevorzugterweise zwei Teilalgorithmen haben, d. h. einen kryptographischen Algorithmus und einen Test-Algorithmus, der ausschließlich daraufhin programmiert ist, daß er ein möglichst "chaotisches" Betriebsverhalten abhängig von unterschiedlichen Eingangsdaten aufweist.

Bei der Berechnung der Ausgangsdaten, die zur Überprüfung der Authentizität der Vorrichtung verwendet werden, werden jedoch die Ergebnisse des Test-Algorithmus nicht berücksichtigt, sondern lediglich die Betriebsdaten, die die elektronische Schaltung aufweist, die den Test-Algorithmus ausführt, und die Ausgangsdaten des Krypto-Algorithmus, was es für einen Fälscher noch schwieriger macht, den Test-Al-

gorithmus anzugreifen, da er im günstigsten Fall lediglich Eingangsdaten in den Test-Algorithmus erfährt, jedoch keine Ausgangsdaten.

Eine weitere Erhöhung der Sicherheit besteht insbesondere darin, einen mehrstufigen Krypto-Algorithmus und ebenfalls einen mehrstufigen Test-Algorithmus zu verwenden, wobei als Eingangsdaten für eine Stufe des Krypto-Algorithmus neben dem Zwischenergebnis der vorausgehenden Stufe des Krypto-Algorithmus auch die Betriebsdaten des Test-Algorithmus, die durch die Ausführung der vorausgehenden Stufe des Test-Algorithmus erzeugt worden sind, verwendet werden. Diese "Verschachtelung" eines mehrstufigen Krypto-Algorithmus mit einem mehrstufigen Test-Algorithmus bietet eine hohe Sicherheit gegen Fälschungen.

Im Gegensatz zu früheren Fälschungsversuchen, die die Struktur eines Chips unter Verwendung verschiedener Verfahren zu identifizieren versucht haben, und die dann diese Daten verwendet haben, um die Funktionalität eines Chips zu analysieren und in einen anderen Chip zu integrieren, bzw. durch einen Computer zu simulieren, müssen Fälscher, die die erfindungsgemäße Vorrichtung angreifen, einen vollständigen Neuentwurf des Chips durchführen und vielleicht sogar das Produktionsverfahren darauf ausrichten. Dies ist notwendig, da nicht nur die Funktionalität des Chips nachgeahmt werden muß, sondern auch das Betriebsverhalten der elektronischen Schaltung, d. h. die Hardware. Im Gegensatz zum Stand der Technik, bei dem die Sicherheit durch immer ausgefeiltere Funktionalitäten zu erreichen versucht wurde, setzt die vorliegende Erfindung darauf, Hardwareaspekte in die Sicherheit miteinzubeziehen, derart, daß ein Fälscher unter Umständen sogar genau den gleichen Prozeß zur Herstellung integrierter Schaltungen verwenden muß, um identische Leistungs- bzw. Laufzeitdaten nachzuahmen, um eine authentische Vorrichtung zu simulieren, d. h. zu fälschen.

Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend bezugnehmend auf die beiliegenden Zeichnungen detaillierter erläutert. Es zeigen:

Fig. 1 eine Prinzipdarstellung einer Vorrichtung gemäß der vorliegenden Erfindung;

Fig. 2 ein bevorzugtes Ausführungsbeispiel gemäß der vorliegenden Erfindung;

Fig. 3 das Zusammenwirken eines Krypto-Algorithmus und eines Test-Algorithmus gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung;

Fig. 4 ein Flußdiagramm für ein Verfahren zum Prüfen der Authentizität unter Verwendung zweier erfindungsgemäßer Vorrichtungen; und

Fig. 5 ein Flußdiagramm eines Verfahrens zum verschlüsselten Übertragen von Informationen von einem ersten Ort zu einem zweiten Ort unter Verwendung zweier erfindungsgemäßer Vorrichtungen.

Fig. 1 zeigt als Prinzipblockschaltbild eine erfindungsgemäße Vorrichtung 10 zum Liefern von Ausgangsdaten 12 als Reaktion auf Eingangsdaten 14, um abhängig von den Ausgangsdaten 12 die Authentizität der Vorrichtung 10 zu bestimmen. Die Vorrichtung 10 umfaßt eine elektronische Schaltung 16 zum Ausführen eines Algorithmus, der aus den Eingangsdaten 14 die Ausgangsdaten 12 erzeugt, und eine Einrichtung 18 zum Erfassen von Betriebsdaten, die durch einen Betrieb der elektronischen Schaltung 16 beeinflußt werden, wobei die Einrichtung 18 zum Erfassen von Betriebsdaten mit der elektronischen Schaltung 16 derart gekoppelt ist, daß die Betriebsdaten der elektronischen Schaltung 16 durch den Algorithmus verwendet werden, um die Ausgangsdaten 12 zu erzeugen.

Die Einrichtung 18 zum Erfassen von Betriebsdaten erfaßt vorzugsweise eine verstrichene Berechnungszeit oder den Leistungsverbrauch der elektronischen Schaltung 16 zum Ausführen eines Algorithmus. Im Gegensatz zu der Funktionalität, die der Algorithmus, der durch die elektronische Schaltung 16 implementiert ist, ausführt, werden die Betriebsdaten auch als Umgebungsdaten bezeichnet. Solche Umgebungsdaten können alle Daten sein, die dazu geeignet sind, den Betrieb eines Chips, d. h. einer elektronischen Schaltung, zu beschreiben, beispielsweise die elektromagnetische Strahlung, die von der elektronischen Schaltung 16 abgegeben wird. Eine Grenze besteht lediglich wegen der technischen Möglichkeiten, Meßeinrichtungen in die Vorrichtung 10 zu integrieren.

Die Vorrichtung 10 ist vorzugsweise in integrierter Form hergestellt und als Smart Card, PC-Card, Telefonkarte, elektronischer Schlüssel und dergleichen ausgeführt. Die Messung der Betriebsdaten durch die Einrichtung 18 findet dann auf der Karte selbst statt. Daher werden Zeitdaten und Leistungsdaten als Betriebsdaten bevorzugt, da sie ohne weiteres meßbar sind.

Die Messung des aktuellen Leistungsverbrauchs kann durch ein relativ einfaches elektronisches Netzwerk realisiert werden, das aus einem Widerstand, einem Kondensator und einem Analog/Digital-Wandler besteht. Diese Schaltungsanordnung sollte so genau als möglich sein. Aufgrund von Schwankungen der Eingangsleistung und der Materialeigenschaften ist die Genauigkeit jedoch begrenzt, da wiederholte Ausführungen mit den gleichen Eingangswerten genau die gleichen Ergebnisse unabhängig von Umgebungsbedingungen erzeugen müssen.

Fig. 2 zeigt eine etwas detailliertere Ansicht der erfindungsgemäßen Vorrichtung 10 gemäß einem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung. Die elektronische

Schaltung 16 zum Ausführen eines Algorithmus ist dabei in zwei Teilschaltungen 16a und 16b unterteilt, wobei die Teilschaltung 16a einen Krypto-Algorithmus ausführen kann, während die Teilschaltung 16b einen Test-Algorithmus ausführen kann.

Die Einrichtung 18 zum Erfassen von Betriebsdaten ist ebenfalls zweigeteilt und umfaßt eine Einrichtung zur Zeitmessung 18a und eine weitere Einrichtung zur Leistungsmessung 18b.

Die Zeitmessung durch die Einrichtung 18 zum Erfassen von Betriebsdaten sollte mittels eines internen Taktchips durchgeführt werden, da ein zugeführter Takt zu stark variieren kann. Die Zeitsteuerung sollte so genau als möglich sein, da wiederholte Ausführungen die gleichen Ergebnisse erzeugen müssen. Zeitmessungen können auf der Basis des Takts des Chips durchgeführt werden, wodurch jedoch sicherheitsrelevante Kompromisse eingegangen werden müssen, da dann die tatsächliche Geschwindigkeit der elektronischen Schaltung 16 relevant ist, sondern nur die Taktzyklen pro Befehl entscheidend sind.

Dadurch, daß Betriebsdaten der Einrichtung 16 verwendet werden, wird der Algorithmus, der durch die Einrichtung 16 ausgeführt wird, Hardware-abhängig gemacht. Gleichzeitig müssen diese Meßwerte jedoch zuverlässig reproduzierbar sein, derart, daß beim Überprüfen der Authentizität aufgrund von Parameterschwankungen keine falschen Ergebnisse auftreten. Andererseits sollten die Anforderungen an die Betriebsdaten, d. h. die Herstellungstoleranzen zum Herstellen einer zu testenden Vorrichtung und einer Prüfvorrichtung, so eng als möglich gewählt werden, um eine hohe Sicherheit zu erreichen.

Bezüglich der Zeitmessung ist die Einrichtung 18a bevorzugterweise angeordnet, um absolute Zeiten mittels eines

unabhängigen Taktchips, der in der Einrichtung 18a integriert ist, zu messen. Damit wird eine höhere Sicherheit erreicht, jedoch auch eine Abhängigkeit von äußeren Taktgebern, wodurch die Portierbarkeit von einem Gerät zu einem anderen verschlechtert wird.

Bei der Einrichtung 18b zur Leistungsmessung entstehen durch die Hardwareabhängigkeit gewisse Probleme. Digitalisierfehler des A/D-Wandlers, der in der Einrichtung 18b zur Leistungsmessung enthalten ist, können die Resultate unvorhersagbar machen. Dieses Problem kann entweder dadurch gelöst werden, daß sehr hohe Abtastraten verwendet werden, und daß großzügige Rundungen durchgeführt werden, oder daß in der Einrichtung 18b zur Leistungsmessung aufwendige Rauschreduktionsalgorithmen implementiert sind. Eine andere Möglichkeit, dieses Problem anzugehen, besteht in der Verwendung von Mustererkennungsalgorithmen, die bestimmte Klassifikationszahlen aus den aufgezeichneten Signalen, d. h. Zeit- oder Leistungsverbrauchswerten, liefern, die durch diesen Mustererkennungsalgorithmus verwendet werden können. In diesem Fall besteht die Hardwareabhängigkeit der Vorrichtung 10 darin, daß nicht absolute Betriebsdaten verwendet werden, sondern bestimmte "Verläufe", d. h. der Leistungsverbrauch über der Zeit, oder bestimmte Berechnungszeiten einzelner Algorithmusstufen eingesetzt werden, um den zusätzlichen Sicherheitsaspekt der Hardwareabhängigkeit zu erreichen.

Bezüglich der Architektur der Verknüpfung des Algorithmus, der durch die elektronische Schaltung 16 ausgeführt wird, und der Betriebsdaten werden lediglich beispielhaft zwei Möglichkeiten erwähnt. Die eine Möglichkeit wird als Prüfpunktarchitektur bezeichnet. Eine externe Steuerung, die mit der Einrichtung 16 beispielsweise über einen Hilfseingang gekoppelt ist, unterbricht die Ausführung des Algorithmus durch die elektronische Schaltung 16 z. B. nach einer bestimmten Anzahl von Taktzyklen oder Sekunden. Dann wird ein "Schnappschuß" des Ausführungszustands der elektronischen

Schaltung 16 genommen. Dieser Schnappschuß umfaßt beispielsweise Daten bezüglich des Algorithmusfortschritts, Registerzustände, den Leistungsverbrauch seit dem letzten Prüfpunkt oder den Zeitverbrauch seit dem letzten Prüfpunkt. Diese Architektur macht es nicht erforderlich, den Algorithmus in Teile aufzuteilen. Wenn jedoch keine Taktzyklen für die Zeitmessung verwendet werden, ist diese Möglichkeit in der Realität schwierig zu implementieren, da eine langsamere Ausführung des Algorithmus aufgrund von äußeren Bedingungen einen Schnappschuß vollständig ändern kann. Ein Schnappschuß kann ferner nicht gerundet werden, wie es bereits angesprochen wurde. In den meisten Fällen werden ferner zu viele Daten gesammelt, daher müssen Daten kombiniert werden. Ein Kombinationsalgorithmus hängt von den während des Schnappschusses aufgezeichneten Daten ab und kann von einer einfachen XOR-Verknüpfung bis zu komplexen Prüfsummenalgorithmen, wie z. B. "Message-Digest-Algorithmen" reichen.

Die zweite Möglichkeit, die als die "Anforderungsarchitektur" bezeichnet wird, wird daher bevorzugt. Dieselbe ist in Fig. 3 schematisch dargestellt. Fig. 3 zeigt die Verschachtelung eines Krypto-Algorithmus 16a mit einem Testalgorithmus 16b. Der Krypto-Algorithmus 16a, der beispielsweise ein DES-Algorithmus sein kann, der in n Stufen aufgeteilt ist, erhält in Stufe 1 die Eingangsdaten 14. Ein Test-Algorithmus 16b, auf den noch eingegangen wird, ist ferner vorzugsweise ebenfalls in n Stufen aufgebaut und enthält in seiner Stufe 1 ebenfalls die Eingangsdaten 14.

Nachdem der Krypto-Algorithmus 16a die erste Stufe ausgerechnet hat, liefert er ein bestimmtes Zwischenergebnis. Die erste Stufe des Test-Algorithmus 16b liefert nicht die Ergebnisse des Test-Algorithmus, die uninteressant sind, sondern die Betriebsdaten desselben als Eingangssignal in die zweite Stufe des Krypto-Algorithmus 16a, wie es durch einen Pfeil 20 dargestellt ist. Dieses Verfahren wiederholt sich für jede der n Stufen, derart, daß jede Stufe des Kryp-

to-Algorithmus 16a als Eingangssignal sowohl das Zwischenergebnis der letzten Stufe des Krypto-Algorithmus als auch die Betriebsdaten des Test-Algorithmus der letzten Stufe erhält. Diese Architektur heißt deswegen Anforderungsarchitektur, da entweder der Krypto-Algorithmus selbst oder eine Steuerung den Test-Algorithmus auffordert, Messungen von Betriebsdaten durchzuführen und die Betriebsdaten dann zum Krypto-Algorithmus zu übermitteln.

Obwohl bisher davon gesprochen wurde, daß, wenn sowohl der Krypto-Algorithmus als auch der Test-Algorithmus durch die elektronische Schaltung 16 ausgeführt werden, die Ergebnisse des Test-Algorithmus nicht berücksichtigt werden, und nur die Betriebsdaten der elektronischen Schaltung, die den Test-Algorithmus ausführt, bei der Erzeugung der Ausgangsdaten 12 berücksichtigt werden, können selbstverständlich auch die Ergebnisdaten des Test-Algorithmus in den Krypto-Algorithmus miteinbezogen werden. Dadurch, daß die Ergebnisdaten des Test-Algorithmus jedoch in der Vorrichtung selbst verworfen werden und überhaupt nicht nach außen treten, wird es einem Fälscher wesentlich schwerer gemacht, auf den Test-Algorithmus zu schließen, um dessen Betriebsverhalten zu simulieren, um die Betriebsdaten zu gewinnen, da er im für ihn günstigsten Fall lediglich die Eingangsdaten 14 in denselben und die Betriebsdaten kennt, jedoch nicht die Ausgangsdaten. Es ist ihm daher nahezu unmöglich, die Funktionalität des Test-Algorithmus nachzubilden, um auf die Betriebsdaten schließen zu können.

Prinzipiell wäre es auch möglich, die Betriebsdaten mit irgend einem anderen Algorithmus zu simulieren, der ähnliche Betriebsverhältnisse aufweist. Wenn jedoch ein Test-Algorithmus mit ausreichender Komplexität verwendet wird, wie z. B. ein Algorithmus zur Berechnung von Fraktalen, so ist es in der Tat nahezu unmöglich, das Betriebsverhalten des Test-Algorithmus ohne Kenntnis der Ergebnisdaten nachzubilden. Selbst wenn die Funktionalität des Test-Algorithmus mit

sehr großem Aufwand aus dem Layout der integrierten Schaltungen, die denselben ausführt, gewonnen werden sollte, so besteht der Sicherheitsaspekt der vorliegenden Erfindung darin, daß die Funktionalität an sich überhaupt nichts nutzt, sondern daß neben der Funktionalität auch das Betriebsverhalten der elektronischen Schaltung 16 nachgebildet werden müßte. Außerdem weiß ein Fälscher a priori nicht, ob nun die Betriebsdaten des Test-Algorithmus in den Krypto-Algorithmus eingespeist werden oder nicht, bzw. welche Kombinationen oder Verknüpfungen derselben vorliegen. So wäre es selbstverständlich möglich, nur bei ein paar Stufen die Ergebnisdaten des Test-Algorithmus zu berücksichtigen, und bei den anderen Stufen lediglich die Betriebsdaten in die Durchführung des Krypto-Algorithmus miteinzubeziehen.

Für die vorliegende Erfindung ist es daher nicht unbedingt notwendig, das Betriebsverhalten des kryptographischen Algorithmus oder Krypto-Algorithmus zu messen. Wie es aus Fig. 3 ersichtlich ist und bereits hinreichend beschrieben worden ist, kann ein Test-Algorithmus durch die elektronische Schaltung 16 ausgeführt werden, der vorzugsweise ein komplexer und schwieriger Algorithmus mit nur schwer vorhersagbarem oder "pseudochaotischem" Verhalten ist. Wenn nun im einfachsten Fall Eingangssignale verschiedener Länge verschiedene Betriebsdaten erzeugen, und wenn der Algorithmus an sich geheimgehalten wird, so ist bereits ein guter Schutz erreicht, da ein Fälscher, der die Funktionalität des Algorithmus nachbilden möchte, keine authentische Karte erzeugen kann, da ja nicht die Ergebnisdaten des Test-Algorithmus die Ausgangsdaten bilden, sondern im einfachsten Fall die Betriebsdaten. Zur Verbesserung der Version mit Test-Algorithmus allein können selbstverständlich bei der Erzeugung der Ausgangsdaten nicht nur ausschließlich die Betriebsdaten verwendet werden, sondern auch die Ergebnisdaten mit den Betriebsdaten auf irgendeine Art und Weise verknüpft werden. Den besten Schutz erreicht man jedoch, wenn der Test-Algorithmus mit dem Krypto-Algorithmus beispielsweise auf die in

Fig. 3 gezeigte Art verknüpft wird.

Der Test-Algorithmus sollte spezielle Merkmale der elektronischen Schaltung 16 benutzen, wodurch die Schwierigkeit für Angriffe weiter erhöht wird. Ferner sollte dieser Algorithmus kein einfaches Laufzeitverhalten zeigen, das darin bestehen könnte, daß höherwertige Eingangssignale in langsameren Berechnungen resultieren. Ein solches Verhalten würde das Betriebsverhalten der elektronischen Schaltung 16, die den Algorithmus ausführt, in gewisser Weise wieder vorhersehbar machen. Daher kann das Eingangssignal beispielsweise mittels einer Serie von XOR-Operationen randomisiert werden, oder dasselbe kann durch eine Funktion mit "pseudo-chaotischem" Verhalten geschickt werden, derart, daß das Ausgangssignal der Funktion zwar definiert mit dem Eingangssignal zusammenhängt, daß dieser Zusammenhang jedoch außerordentlich kompliziert ist und allein durch Betrachten kein funktionsmäßiger Zusammenhang zu sehen ist. In diesem Fall besteht der Test-Algorithmus selbst aus zwei Teilen, und zwar aus einem Teil, der das Eingangssignal zufällig oder zumindest sehr unvorhersagbar macht und aus einem zweiten Teil, der der eigentliche Test-Algorithmus ist, um beispielsweise den Zeitablauf oder den Leistungsverbrauch der integrierten Schaltung 16 bestimmen zu können.

Fig. 4 zeigt ein Flußdiagramm für ein Verfahren zum Überprüfen der Authentizität einer Vorrichtung, wie es beispielsweise ein elektronisches Türschloß ausführen könnte, um nur einen Inhaber einer authentischen "Schlüsselkarte" durch die Türe passieren zu lassen. Ein solches elektronisches Türschloß umfaßt im allgemeinen Fall eine Mikrosteuerung und ein Karten-Lese/Schreib-Gerät, in das eine Karte mit der erfindungsgemäßen Vorrichtung eingeführt werden kann, sowie ein festinstalliertes Karten-Lese/Schreib-Gerät, in dem eine Referenzkarte, die ebenfalls die erfindungsgemäße Vorrichtung aufweist, fest eingebaut und von außen unzugänglich angeordnet ist. Die Referenz-

oder Prüfvorrichtung entspricht der zu testenden Vorrichtung dahingehend, daß beide beispielsweise aus einer gleichen Produktcharge stammen, um sich hardwaremäßig zu gleichen, um ein möglichst ähnliches Betriebsverhalten zu haben.

Möchte nun ein Karteninhaber in eine Tür eintreten, die durch ein derartiges elektronisches Schlüsselsystem versehen ist, so wird er seine Karte, auf der die erfindungsgemäße Vorrichtung angebracht ist, in das Kartenlesegerät einführen.

Das Verfahren zum Überprüfen der Authentizität der eingeführten, d. h. zu testenden Vorrichtung ist in Fig. 4 dargestellt. Zunächst wählt die Mikrosteuerung beliebige zufällige Eingangsdaten (Block 40). In einem nächsten Schritt werden diese Eingangsdaten sowohl in die zu testende Vorrichtung als auch in die Prüfvorrichtung eingespeist (Block 42). Sowohl die von dem Benutzer bezüglich ihrer Authentizität zu überprüfende Vorrichtung, d. h. die zu testende Vorrichtung, als auch die in dem Türschloß vorzugsweise fest eingebaute Prüfvorrichtung führen nun parallel zueinander die gleichen Schritte durch und erzeugen Ausgangsdaten, wobei die Ausgangsdaten der Prüfvorrichtung von den Betriebsdaten der elektronischen Schaltung 16 der Prüfvorrichtung abhängen, und wobei die Ausgangsdaten der zu testenden Vorrichtung von den Betriebsdaten der elektronischen Schaltung 16 der zu testenden Vorrichtung abhängen.

In einem Block 44 werden die Ausgangsdaten der beiden Vorrichtungen verglichen. Stimmen dieselben überein, so wird die Authentizität der zu testenden Vorrichtung bejaht (Block 46). Stimmen die Ausgangsdaten nicht überein, so wird die Authentizität der zu testenden Vorrichtung verneint (Block 48), und das Türschloß wird nicht geöffnet. In diesem Fall werden sowohl die zu testende Vorrichtung als auch die Prüfvorrichtung von ein und derselben Mikrosteuerung "bedient". Dies bedeutet, daß beispielsweise ein externer Takt zur Mes-

sung des Zeitverhaltens, der mit der Einrichtung 18 zum Erfassen der Betriebsdaten gekoppelt ist, für beide Vorrichtungen identisch sind. In diesem Fall können die Betriebsdaten außerordentlich genau ermittelt werden, da Taktschwankungen oder ähnliches beide Vorrichtungen gleichermaßen betreffen und somit nicht zu einer Divergenz der beiden Vorrichtungen führen.

Dieses Verfahren, das darin besteht, daß einer Vorrichtung ein Eingangssignal gegeben wird, derart, daß dieselbe ein Ausgangssignal erzeugt, wobei das Ausgangssignal in Abhängigkeit des Eingangssignals beurteilt wird, wird auch als "Challenge-Response"-Algorithmus bezeichnet. Vorzugsweise wird irgendein zufälliges Eingangssignal der Vorrichtung zugeführt, welche dann mittels der elektronischen Schaltung 16 ein Ergebnis berechnet und die gesammelten Betriebsdaten ausgibt, d. h. bei den Ausgangsdaten verarbeitet. Die Verifizierung findet durch Vergleich mit einer Referenz- oder Prüfvorrichtung statt. Für einen Angreifer wäre es prinzipiell möglich, die Datenkommunikation zwischen der zu testenden Vorrichtung und der Mikrosteuerung innerhalb des Kartenlesegeräts, das ja per Definition nach außen zugänglich sein muß, abzuhören. Da jedoch bei dem bevorzugten Ausführungsbeispiel der vorliegenden Erfindung, das in Fig. 3 dargestellt ist, die Betriebsdaten lediglich innerhalb der erfindungsgemäßen Vorrichtung verarbeitet werden und nicht nach außen übermittelt werden, und da ferner die Ergebnissdaten des Test-Algorithmus ebenfalls innerhalb der Vorrichtung verbleiben und nicht nach außen übermittelt werden, und sogar überhaupt nicht weiter berücksichtigt werden, wird einem Angreifer auf die erfindungsgemäße Vorrichtung auch ein Abhören nicht besonders viel weiterhelfen. Die erfindungsgemäße Vorrichtung umfaßt daher drei Geheimaspekte, die zunächst ein herkömmliches geheimes Passwort für den Krypto-Algorithmus, weiterhin den geheimen Test-Algorithmus und schließlich den konkreten Hardware-Entwurf der elektronischen Schaltung 16 umfassen.

Das in Fig. 3 gezeigte Konzept des Einspeisens der Betriebsdaten in entsprechende folgende Stufen eines Krypto-Algorithmus, der bei dem bevorzugten Ausführungsbeispiel der DES-Algorithmus ist, führt zu dem sicherheitsmäßig bevorzugten Verwenden von Einbahnstraßen-Funktionen. Dies bedeutet, daß von bestimmten Eingangsdaten lediglich Ausgangsdaten berechnet werden können, daß jedoch nicht von den Ausgangsdaten funktionsmäßig auf die Eingangsdaten zurückgerechnet werden kann, da die Verwendung der Betriebsdaten eine chronologische Reihenfolge der Berechnung festlegt. Bei der in Fig. 4 gezeigten Überprüfung der Authentizität einer zu testenden Vorrichtung ist eine Umkehrung der Funktionalität auch gar nicht erforderlich, da sowohl die zu testende Vorrichtung als auch die Prüfvorrichtung parallel eine Einbahnstraßen-Funktion durchführen und niemals eine umgekehrte Berechnungsreihenfolge einsetzen müssen.

Wenn für die elektronische Schaltung 16 spezielle Prozessoren eingesetzt werden, die für bestimmte Operationen optimiert sind, derart, daß ein Standardchip oder ein Computer nicht in der Lage ist, das Zeitverhalten bestimmter Prozessoren zu simulieren, kann die Sicherheit weiter gesteigert werden.

Eine weitere Verbesserung besteht darin, daß der Test-Algorithmus, dessen Ergebnisse bei dem bevorzugten Ausführungsbeispiel, das in Fig. 3 gezeigt ist, nicht verwendet werden, und der lediglich zur Erzeugung der Betriebsdaten vorhanden ist, von Zeit zu Zeit ausgetauscht werden kann. Ein solcher Austausch des Test-Algorithmus ist flexibel möglich, es muß lediglich darauf geachtet werden, daß die zu testende Vorrichtung und die Prüfvorrichtung denselben Test-Algorithmus haben, um bei authentischer Karte gleiche Betriebsdaten zu haben.

Die vorliegende Erfindung kann auf nahezu jeden kryptogra-

phischen Algorithmus, d. h. Krypto-Algorithmus, angewendet werden. Ein Vorteil der vorliegenden Erfindung besteht zusätzlich darin, daß die vorliegende Erfindung in bestehende Sicherheitssysteme integriert werden kann.

Fig. 5 zeigt eine weitere Anwendungsmöglichkeit der erfindungsgemäßen Vorrichtung am Beispiel des verschlüsselten Übertragens von Informationen von einem Ort zu einem anderen Ort, wie es beispielsweise beim "Fernsehen gegen Bezahlung" oder "Pay-TV" zu finden ist. Zunächst müssen die zu verschlüsselnden Informationen in einem Sender verschlüsselt werden. Dazu umfaßt der Sender eine Smart Card, die eine erfindungsgemäße Vorrichtung aufweist. Zunächst werden vom Sender zufällige Eingangsdaten als Passwort-Zeichenkette ausgewählt (Block 50). In einem Block 52 werden die Eingangsdaten 14 in die Sender-Smart Card eingespeist, die in einem Schritt 54 Ausgangsdaten 12 erzeugt. Die zu verschlüsselnden Informationen werden nun mit den von der Sender-Smart Card erzeugten Ausgangsdaten 12 als Schlüssel verschlüsselt (Block 56). Die verschlüsselten Informationen werden nun zusammen mit den im Block 50 ausgewählten Ausgangsdaten von dem einen Ort zu dem anderen Ort, d. h. von dem Sender zu dem Empfänger, übertragen (Block 58).

Es sei darauf hingewiesen, daß zum einen nun die Informationen verschlüsselt sind und daher nur von dem entschlüsselt werden, der eine entsprechende Autorisierung beispielsweise in Form einer Empfänger-Smart Card erworben hat. Zum anderen wird der Schlüssel zum Verschlüsseln der Informationen nicht explizit übertragen, sondern lediglich die Eingangsdaten in die Sender-Smart Card. Ein Nutzer, der nicht im Besitz einer autorisierten Empfänger-Smart Card ist, die die gleichen Betriebsdaten wie die Sender-Smart Card aufweist, wird nun nicht in der Lage sein, aus den Eingangsdaten 14 die korrekten Ausgangsdaten 12 zu erzeugen, um die verschlüsselten Informationen wieder zu entschlüsseln.

Zunächst besteht die Aufgabe im Empfänger darin, die Eingangsdaten aus der Übertragung, die sowohl die verschlüsselten Informationen als auch die Eingangsdaten aufweist, zu extrahieren (Block 60). Die in dem Block 60 extrahierten Eingangsdaten werden nun in die Empfänger-Smart Card eingespeist (Block 62), die im Falle einer authentischen Empfänger-Smart Card das gleiche Betriebsverhalten wie die Sender-Smart Card aufweist, und damit aus den Eingangsdaten die gleichen Ausgangsdaten erzeugt (Block 64). In einem Block 66 werden schließlich die verschlüsselten Informationen unter Verwendung der Ausgangsdaten der Empfänger-Smart Card entschlüsselt.

Ist die Empfänger-Smart Card eine gefälschte Karte, die nicht dasselbe Betriebsverhalten wie die Sender-Smart Card aufweist, so wird dies bei dem in Fig. 5 gezeigten Verfahren nicht sofort erkannt, da keine Überprüfung der Authentizität, wie bei Fig. 4, stattfindet. Die Ausgangsdaten, die als Schlüssel zum Entschlüsseln benötigt werden, werden jedoch nicht den Ausgangsdaten, die im Block 54 zum Verschlüsseln verwendet wurde, entsprechen, weshalb keine korrekte Entschlüsselung der verschlüsselten Informationen möglich ist. Dies bedeutet, daß im einfachsten Fall eine gefälschte Smart Card im Empfänger nicht sofort beanstandet wird, sondern daß sie aufgrund anderer Betriebsdaten wie die Sender-Smart Card zwar Ausgangsdaten 12 liefert, daß jedoch mit den gelieferten Ausgangsdaten keine korrekte Entschlüsselung möglich ist, wodurch ein Fälscher keinen Nutzen seiner gefälschten Karte hat.

Die vorliegende Erfindung umfaßt daher eine elektronische Schaltung, die vorzugsweise integriert ist, und eine Einrichtung zum Überwachen des Betriebs der elektronischen Schaltung durch Messen von Daten, wobei der Betrieb der elektronischen Schaltung das Ausführen eines Algorithmus umfaßt, der als Ergebnis einer vorzugsweise komplexen Be-

rechnung Ausgangsdaten liefert. Diese Ausgangsdaten werden jedoch durch die gemessenen Betriebsdaten beeinflusst. Vorzugsweise umfassen die gemessenen Daten Zeit- oder Leistungsmeßdaten. Die erfindungsgemäße Vorrichtung kann beliebig auf Karten, z. B. Smart Cards oder PC-Cards, elektronischen Schlüsseln und dergleichen, untergebracht werden.

PATENTANSPRÜCHE

1. Vorrichtung (10) zum Liefern von Ausgangsdaten (12) als Reaktion auf Eingangsdaten (14), um abhängig von den Ausgangsdaten (12) die Authentizität der Vorrichtung (10) zu bestimmen, mit folgenden Merkmalen:

einer elektronischen Schaltung (16) zum Ausführen eines Algorithmus, der aus den Eingangsdaten (14) die Ausgangsdaten (12) erzeugt; und

einer Einrichtung (18) zum Erfassen von Betriebsdaten, die durch einen Betrieb der elektronischen Schaltung (16) beeinflußt werden,

wobei die Einrichtung (18) zum Erfassen mit der elektronischen Schaltung (16) derart gekoppelt ist, daß die Betriebsdaten der elektronischen Schaltung durch den Algorithmus, der durch die elektronische Schaltung (16) ausgeführt wird, verwendet werden, um die Ausgangsdaten (12) zu erzeugen.

2. Vorrichtung (10) nach Anspruch 1, bei der die Betriebsdaten aus der Gruppe ausgewählt sind, die Zeitdaten und Leistungsdaten umfaßt.
3. Vorrichtung (10) nach Anspruch 1 oder 2, bei der die elektronische Schaltung (16) und die Einrichtung (18) zum Erfassen als eine Einheit integriert sind.
4. Vorrichtung (10) nach einem der vorhergehenden Ansprüche, die in einer Smart Card oder einer PC-Card enthalten ist.
5. Vorrichtung (10) nach einem der vorhergehenden Ansprüche, bei der die elektronische Schaltung (16) angeordnet ist, um einen Krypto-Algorithmus auszuführen.

6. Vorrichtung (10) nach einem der Ansprüche 1 bis 4, bei der die elektronische Schaltung (16) angeordnet ist, um einen Prüfsummen-Algorithmus auszuführen.
7. Vorrichtung (10) nach Anspruch 5, bei der der Krypto-Algorithmus ein mehrstufiger Algorithmus ist, wobei die Betriebsdaten einer Algorithmus-Stufe als Eingangsdaten für die darauffolgende Algorithmus-Stufe verwendet werden.
8. Vorrichtung (10) nach einem der Ansprüche 1 bis 6, bei der die elektronische Schaltung (16) angeordnet ist, um nach einer vorbestimmten Ausführungszeit während der Ausführung des Algorithmus den Betrieb anzuhalten, und bei der die Einrichtung (18) zum Erfassen angeordnet ist, um Betriebsdaten zu der vorbestimmten Ausführungszeit in den Algorithmus einzuspeisen.
9. Vorrichtung (10) nach einem der Ansprüche 1 bis 3, bei der der Algorithmus derart gestaltet ist, daß er die Eingangsdaten (14) zunächst randomisiert, wodurch die Abhängigkeit der Betriebsdaten von den Eingangsdaten pseudozufällig ist.
10. Vorrichtung (10) nach Anspruch 9, bei der die Ausgangsdaten, die durch den Algorithmus erzeugt werden, lediglich die Betriebsdaten sind.
11. Vorrichtung (10) nach einem der Ansprüche 1 bis 4, bei der die elektronische Schaltung (16) zwei Teilschaltungen (16a, 16b) aufweist, die je einen Teil-Algorithmus ausführen, wobei der erste Teil-Algorithmus ein Test-Algorithmus ist, dessen Betriebsdaten durch die Einrichtung (18) zum Erfassen erfaßt werden, und wobei der zweite Teil-Algorithmus ein Krypto-Algorithmus oder ein Prüfsummen-Algorithmus ist, wobei die Betriebsdaten des

Test-Algorithmus in dem Krypto-Algorithmus verarbeitet werden.

12. Vorrichtung (10) nach Anspruch 11, bei der die zweite Teilschaltung (16a) angeordnet ist, um den DES-Algorithmus auszuführen, der n Stufen aufweist, und bei der die erste Teilschaltung (16b) angeordnet ist, um einen Test-Algorithmus auszuführen, der ebenfalls n Stufen aufweist, wobei die Eingangsdaten sowohl in die erste Stufe des DES-Algorithmus als auch in die erste Stufe des Test-Algorithmus einspeisbar sind, und wobei Daten, die in eine weitere Stufe des DES-Algorithmus einspeisbar sind, Ergebnisdaten der ersten Stufe des DES-Algorithmus und Betriebsdaten der ersten Stufe des Test-Algorithmus sind, während ein Ergebnis einer Stufe des Test-Algorithmus verworfen wird.
13. Vorrichtung (10) nach einem der vorhergehenden Ansprüche, bei der die Einrichtung zum Erfassen von Betriebsdaten eine Zeitmeßeinrichtung (18a) und eine Leistungsmeßeinrichtung (18b) aufweist, um die Zeit zu messen, die die elektronische Schaltung (16) zum Ausführen einer bestimmten Aufgabe benötigt, bzw. um die Leistung zu messen, die beim Ausführen der bestimmten Aufgabe verbraucht wird.
14. Vorrichtung (10) nach Anspruch 13, bei der die Leistungsmeßeinrichtung (18b) einen Widerstand, einen Kondensator und einen A/D-Wandler zum Messen der verbrauchten Leistung aufweist.
15. Vorrichtung (10) nach Anspruch 13 oder 14, bei der die Zeitmeßeinrichtung einen internen Taktgenerator aufweist.
16. Vorrichtung (10) nach einem der vorhergehenden Ansprüche, bei der die Einrichtung (18) zum Erfassen der Be-

triebsdaten einen Mustererkennungs-Algorithmus aufweist, um aus Leistungs- oder Zeitparametern der elektronischen Schaltung (16) die Betriebsdaten zu erzeugen.

17. Verfahren zum Überprüfen der Authentizität einer zu testenden Vorrichtung (10) gegenüber einer Prüfvorrichtung (10) wobei die zu testende Vorrichtung (10) und die Prüfvorrichtung (10) jeweils eine elektronische Schaltung (16) zum Ausführen eines Algorithmus, der aus Eingangsdaten (14) Ausgangsdaten (12) erzeugt, und eine Einrichtung (18) zum Erfassen von Betriebsdaten, die durch einen Betrieb der elektronischen Schaltung (16) beeinflußt werden, aufweist, wobei die Einrichtung (18) zum Erfassen der Betriebsdaten mit der elektronischen Schaltung (16) derart gekoppelt ist, daß die Betriebsdaten der elektronischen Schaltung durch den Algorithmus verwendet werden, um die Ausgangsdaten zu erzeugen, wobei das Verfahren folgende Schritte aufweist:

Auswählen (40) von Eingangsdaten;

Einspeisen (42) der Eingangsdaten in die zu testende Vorrichtung (10);

Einspeisen (42) der Eingangsdaten in die Prüfvorrichtung (10);

Vergleichen (44) der Ausgangsdaten der zu testenden Vorrichtung mit den Ausgangsdaten der Prüfvorrichtung; und

Bejahen (46) der Authentizität der zu testenden Vorrichtungen gegenüber der Prüfvorrichtung, wenn die Ausgangsdaten übereinstimmen, derart, daß eine Authentizität lediglich bejaht wird, wenn die Betriebsdaten der zu testenden Vorrichtung und der Prüfvorrichtung entsprechend sind.

18. Verfahren zum verschlüsselten Übertragen von Informationen von einem ersten zu einem zweiten Ort, mit folgenden Merkmalen:

Erzeugen (50) eines Zufallsworts;

Einspeisen (52) des Zufallsworts in eine erste Vorrichtung (10) nach einem der Ansprüche 1 bis 16, die an dem ersten Ort angeordnet ist;

Erzeugen (54) der Ausgangsdaten, die von den Betriebsdaten der ersten Vorrichtung (10) abhängen;

Verschlüsseln (56) der Informationen mit den erzeugten Ausgangsdaten als Schlüssel;

Übertragen (58) der verschlüsselten Informationen und des Zufallsworts von dem ersten Ort zu dem zweiten Ort;

Einspeisen (62) des Zufallsworts in eine zweite Vorrichtung (10) nach einem der Ansprüche 1 bis 16;

Erzeugen (64) von Ausgangsdaten durch die zweite Vorrichtung, die an dem zweiten Ort positioniert;

Entschlüsseln (66) der verschlüsselten Informationen unter Verwendung der Ausgangsdaten der zweiten Vorrichtung (10) als Schlüssel,

wobei die entschlüsselten Informationen dann den ursprünglichen Informationen vor dem Verschlüsseln entsprechen, wenn die Betriebsdaten der ersten Vorrichtung (10) an dem ersten Ort den Betriebsdaten der zweiten Vorrichtung (10) an dem zweiten Ort entsprechen.

VORRICHTUNG ZUM LIEFERN VON AUSGANGSDATEN ALS REAKTION AUF
EINGANGSDATEN UND VERFAHREN ZUM ÜBERPRÜFEN DER AUTHENTIZITÄT
UND VERFAHREN ZUM VERSCHLÜSSELN ÜBERTRAGEN VON
INFORMATIONEN

Zusammenfassung

Eine Vorrichtung (10) zum Liefern von Ausgangsdaten (12) als Reaktion auf Eingangsdaten (14), um abhängig von den Ausgangsdaten (12) die Authentizität der Vorrichtung zu bestimmen, umfaßt eine elektronische Schaltung (16) zum Ausführen eines Algorithmus, der aus den Eingangsdaten (14) die Ausgangsdaten (12) erzeugt, und eine Einrichtung (18) zum Erfassen von Betriebsdaten, die durch einen Betrieb der elektronischen Schaltung (16) beeinflußt werden. Die Einrichtung (18) zum Erfassen der Betriebsdaten ist mit der elektronischen Schaltung (16) derart gekoppelt, daß die Betriebsdaten der elektronischen Schaltung (16) durch den Algorithmus verwendet werden, um die Ausgangsdaten (12) zu erzeugen. Die Sicherheit der erfindungsgemäßen Vorrichtung wird dadurch erhöht, daß ein potentieller Fälscher nicht nur die Funktionalität der Vorrichtung, sondern auch Hardware-Aspekte der Vorrichtung, wie z. B. den Leistungsverbrauch oder das Zeitverhalten, nachbilden muß, um eine authentische Karte zu simulieren.

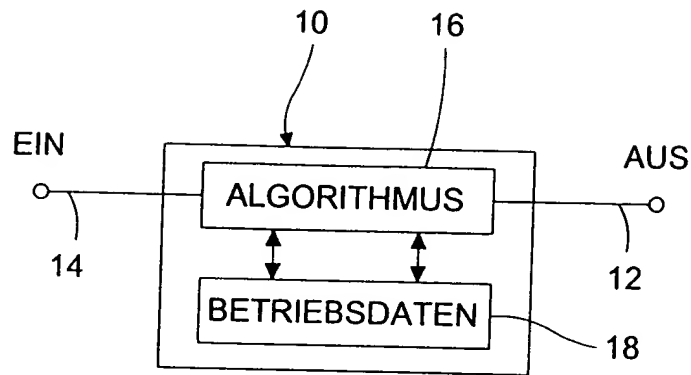


FIG.1

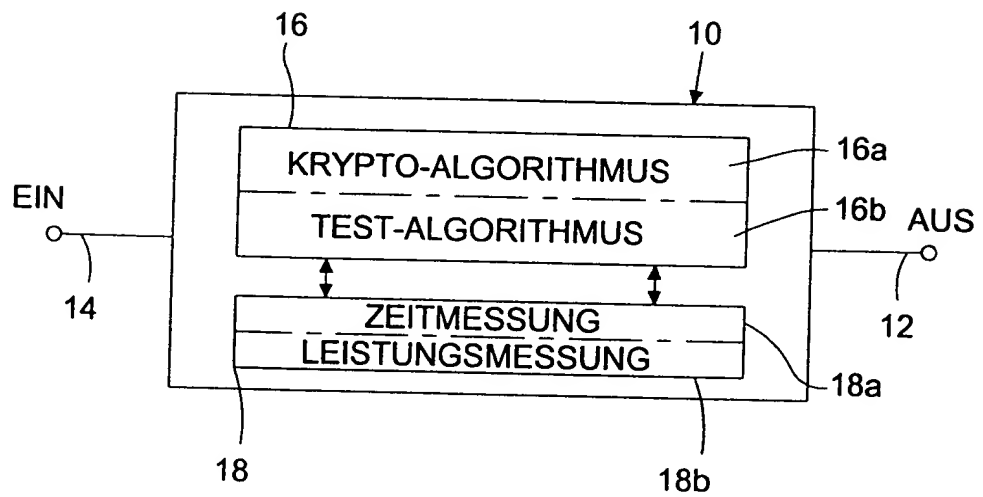


FIG.2

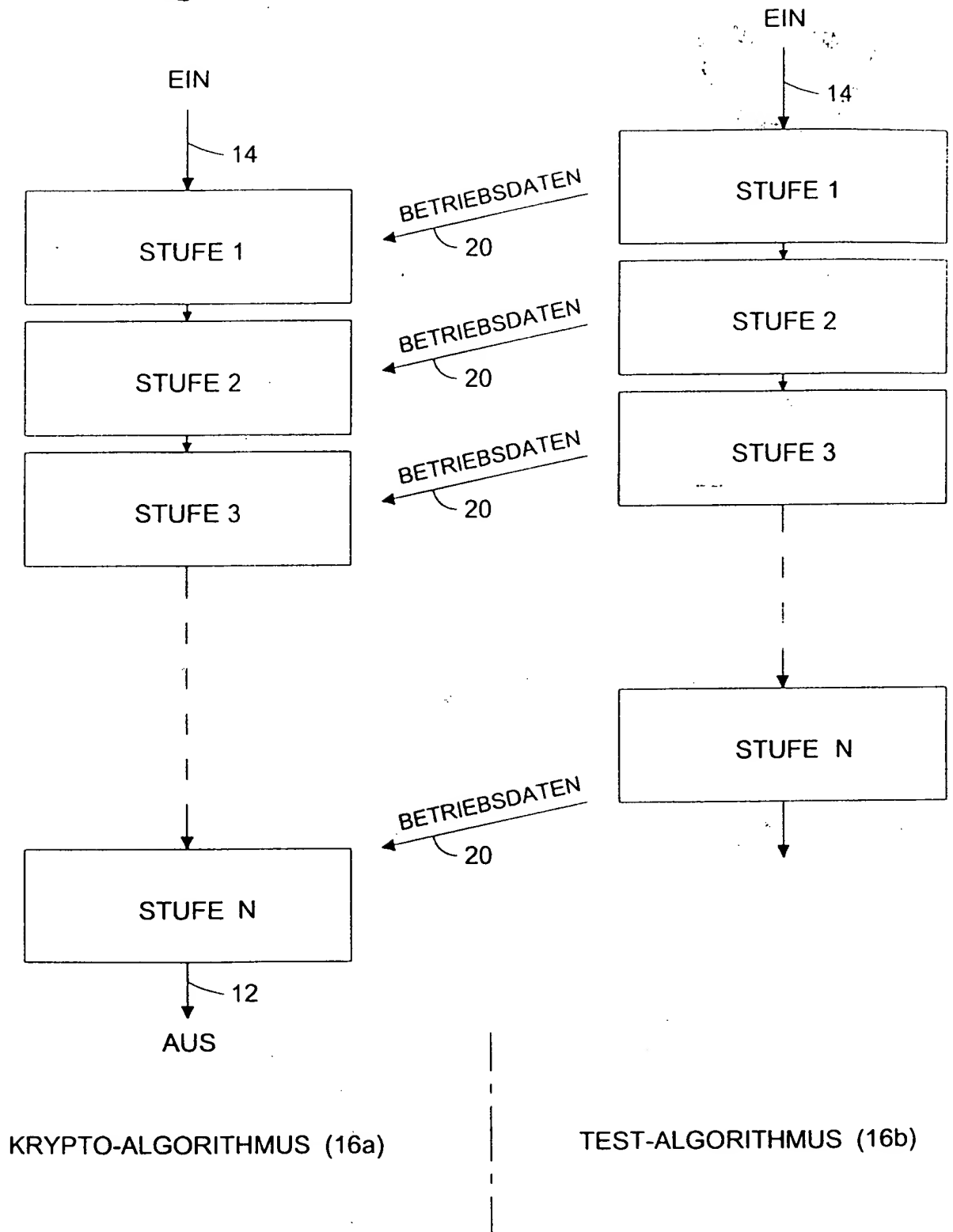


FIG.3

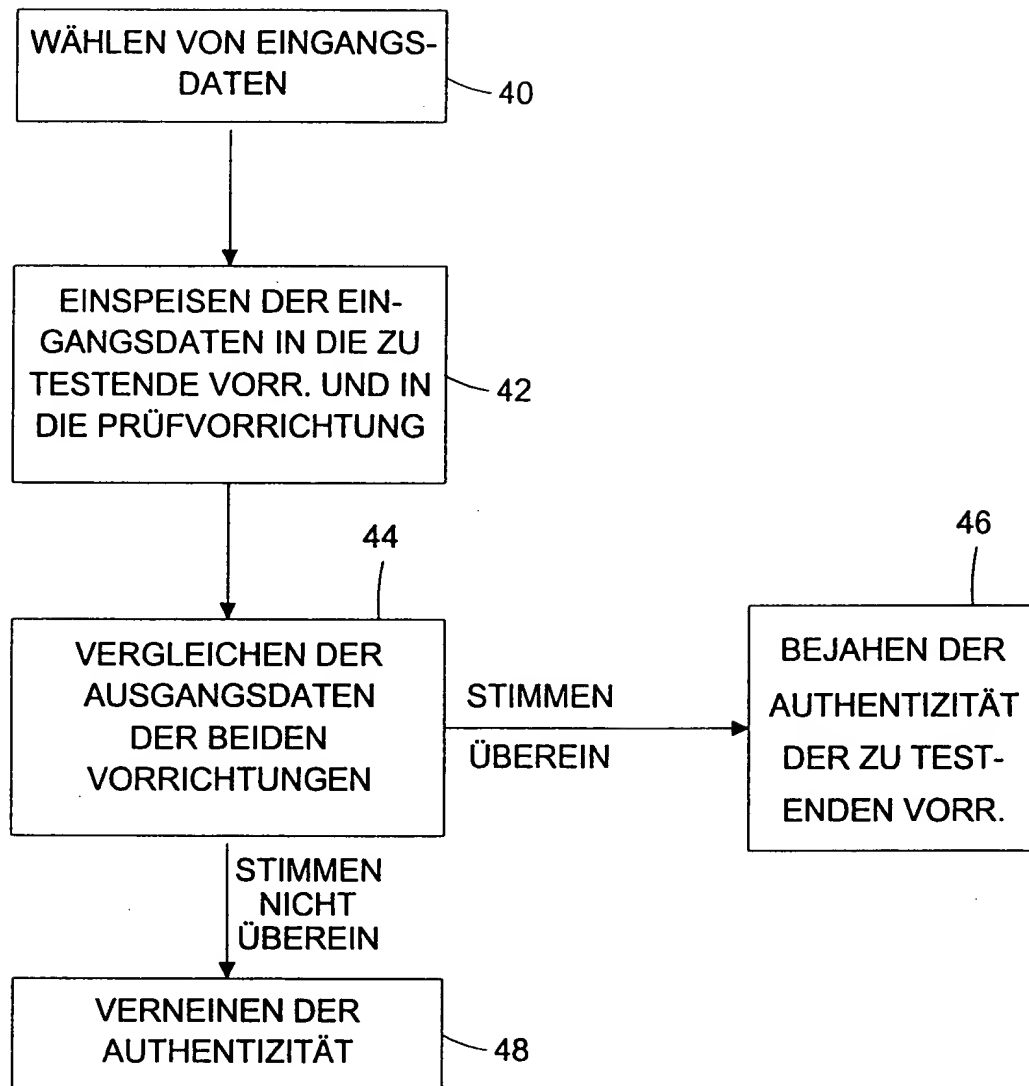


FIG.4

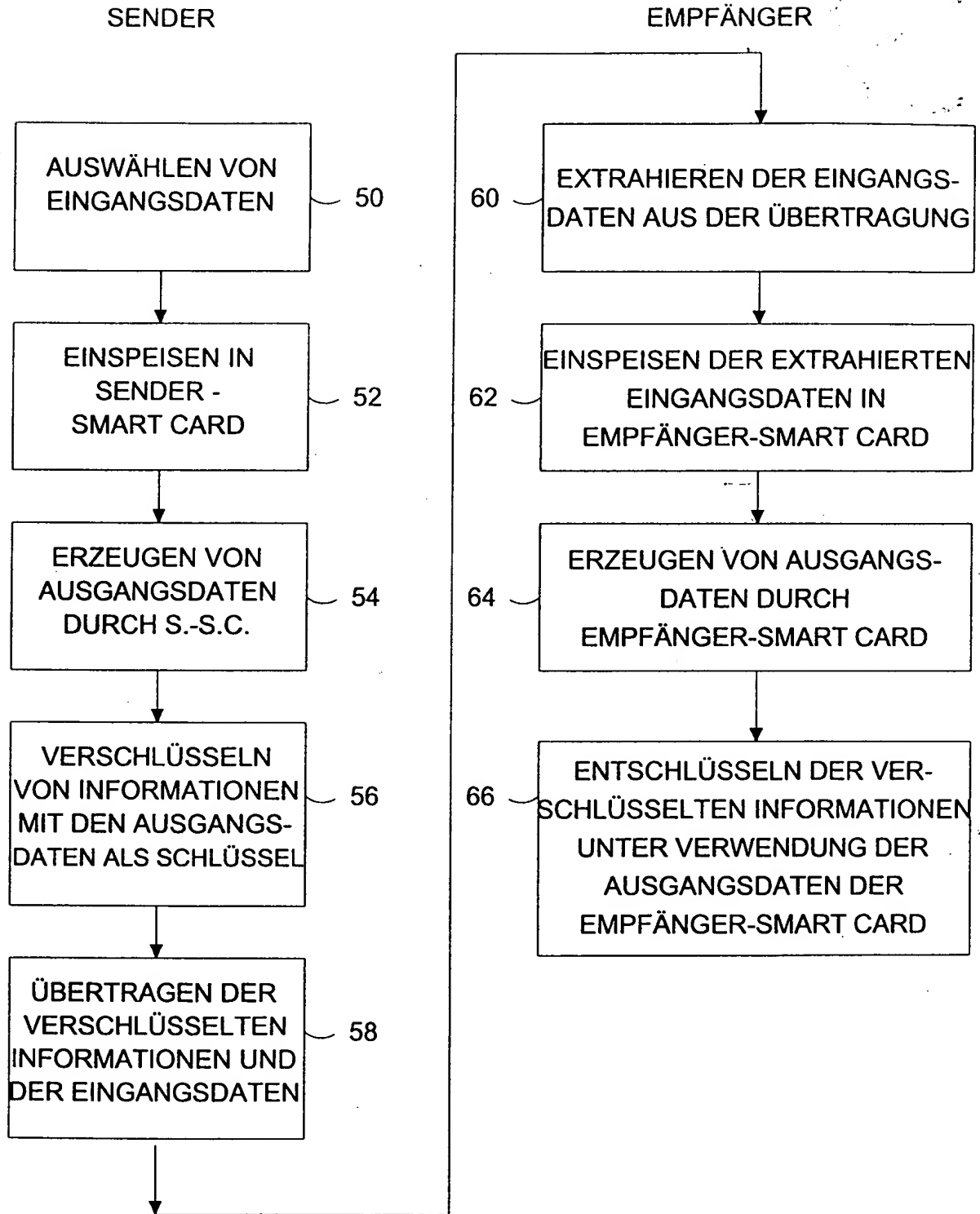


FIG.5

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN
PRÜFUNG BEAUFTRAGTE BEHÖRDE

International
Preliminary
Examination
Report

PC

MITTEILUNG ÜBER DIE ÜBERSENDUNG
DES INTERNATIONALEN VORLÄUFIGEN
PRÜFUNGSBERICHTS
(Regel 71.1 PCT)

An:

SCHOPPE, Fritz
SCHOPPE, ZIMMERMANN & STÖCKELER
Postfach 71 08 67
81458 München
ALLEMAGNE

Absendedatum
(Tag/Monat/Jahr)

16. 11. 00

Aktenzeichen des Anmelders oder Anwalts
FH990804PCT

WICHTIGE MITTEILUNG

Internationales Aktenzeichen
PCT/EP99/06312

Internationales Anmeldedatum (Tag/Monat/Jahr)
27/08/1999

Prioritätsdatum (Tag/Monat/Jahr)
22/09/1998

Anmelder

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG... et al.

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Prüfungsbericht, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.
2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.
3. Auf Wunsch eines ausgewählten Amtes wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

4. ERINNERUNG

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Prüfungsbericht enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Name und Postanschrift der mit der internationalen Prüfung
beauftragten Behörde



Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Schießl, W-P

Tel. +49 89 2399-2860



VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts FH990804PCT	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP99/06312	Internationales Anmeldedatum (Tag/Monat/Jahr) 27/08/1999	Prioritätsdatum (Tag/Monat/Jahr) 22/09/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G07F7/10		
Anmelder FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG... et al.		



1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 10 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☐ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 06/04/2000	Datum der Fertigstellung dieses Berichts 16. 11. 00
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Kampka, A Tel. Nr. +49 89 2399 2244 

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1,2,4-20	ursprüngliche Fassung			
3,3a-3b	eingegangen am	02/08/2000	mit Schreiben vom	02/08/2000

Patentansprüche, Nr.:

1-18	eingegangen am	02/08/2000	mit Schreiben vom	02/08/2000
------	----------------	------------	-------------------	------------

Zeichnungen, Blätter:

1/4-4/4	ursprüngliche Fassung
---------	-----------------------

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen Behörde in der Sprache: , zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, dass das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, dass die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1 - 18
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1 - 18
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1 - 18
	Nein: Ansprüche	

2. Unterlagen und Erklärungen
siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Art. 35(2) PCT hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf die folgenden Dokumente verwiesen:

- D1: EP-A-0 313 967 (GAO GES AUTOMATION ORG) 3. Mai 1989 (1989-05-03)
- D2: EP-A-0 654 919 (SIEMENS AG) 24. Mai 1995 (1995-05-24)
- D3: W. RANKL & W. EFFING: 'Handbuch der Chipkarten' 10. Februar 1998 (1998-02-10), CARL HANSER VERLAG, MÜNCHEN WIEN XP002127583 022759

Der wesentliche Unterschied zwischen dem Konzept der D1 und dem Konzept der Erfindung besteht darin, daß gemäß D1 die individuellen Kenndaten des Speichers 53 immer die gleichen sind, völlig unabhängig von der in die Karte 51 eingespeisten Zufallszahl. Bei der Erfindung ist es jedoch wesentlich, daß die Betriebsdaten der Schaltung eben von den Eingangsdaten der Schaltung abhängen. Dokument D1 offenbart keine Einrichtung zum Erfassen von Betriebsdaten der elektronischen Schaltung, die durch einen Betrieb der elektronischen Schaltung beeinflußt werden, wenn die elektronische Schaltung den Algorithmus ausführt. Darüberhinaus hängen bei D1 die individuellen Speicherdaten nicht von den Eingangsdaten, d.h. der Zufallszahl, welche vom Block Z in Fig. 11 zum Block RN übertragen wird, ab. Dokument D1 offenbart somit auch keine Einrichtung zum Erfassen von Betriebsdaten der elektronischen Schaltung (die Betriebsdaten der Einrichtung 60 in Fig. 11 werden nicht erfaßt, der Speicher 52 ist kein Element, das abhängig von Eingangsdaten in die Karte Ausgangsdaten aus der Karte erzeugt). D1 offenbart ferner nicht, daß die erfaßten Betriebsdaten der elektronischen Schaltung von dem Algorithmus, der durch die elektronische Schaltung ausgeführt wird, verwendet werden, da solche Betriebsdaten der elektronischen Schaltung gar nicht erfaßt werden.

Ausgehend von der D1 besteht die Aufgabe darin, ein Konzept zum verbesserten Schutz von elektronischen Schaltungen zu schaffen und somit eine

fälschungssichere Überprüfung der Authentizität solcher elektronischen Schaltungen und eine fälschungssichere Autorisierung eines Inhabers solcher elektronischer Schaltungen zu schaffen.

Diese Aufgabe wird erfindungsgemäß durch eine Vorrichtung nach Anspruch 1 bzw. ein Verfahren nach Anspruch 17 oder 18 gelöst.

Die in den unabhängigen Ansprüchen definierte Lösung beruht auf einer erfinderischen Tätigkeit: es werden nicht, wie in D1, individuelle Kenndaten irgendeiner elektronischen Schaltung verwendet, sondern die Betriebsdaten genau der elektronischen Schaltung, die abhängig von Eingangsdaten Ausgangsdaten erzeugt. Nach dem erfindungsgemäßen Konzept wird vom Speichern von irgendwelchen Kenndaten in einer Zentrale Abstand genommen.

D1 lehrt von der erfindungsgemäßen Lösung weg, weil hier die individuellen Kenndaten des Speichers immer die gleichen sind und deshalb zu Anfang abgespeichert werden können, während erfindungsgemäß die Betriebsdaten von den Eingangsdaten abhängen, so daß eine einmalige Abspeicherung der Betriebsdaten überhaupt keinen Sinn machen würde. D2 und D3 liegen vom Gegenstand der vorliegenden Erfindung noch weiter ab als D1. Zwar wird hier ausführlicher auf verschiedene Authentisierungsverfahren zwischen Sender und Empfänger eingegangen, jedoch gibt es keinerlei Anregung, bei Ausgangsdaten der Karte, die autorisiert werden soll, deren technologischen Betriebsverhalten hineinspielen zu lassen.

Zur gewerblichen Anwendbarkeit ist nichts einzuwenden.

Somit dürften die unabhängigen Ansprüche 1, 17 und 18 die in Artikel 33(1) PCT genannten Kriterien der Neuheit, erfinderischen Tätigkeit und gewerblichen Anwendbarkeit erfüllen. Die Ansprüche 2 - 16 betreffen vorteilhafte Ausgestaltungen und erfüllen daher ebenfalls die genannten Kriterien.

Der Anmelder beantragte die einteilige Fassung für Anspruch 1, weil seines Erachtens eine Abgrenzung gegenüber D1 zu einem schwerer verständlichen Anspruch führen würde. Da aus der ausführlichen Diskussion der D1 in der

Beschreibung klar ersichtlich ist, welche Merkmale des Anspruchs 1 aus dem Stand der Technik schon bekannt sind, wird gemäß den Richtlinien PCT/GL/3, III, 2.3a im vorliegenden Fall nicht auf der zweiteiligen Anspruchsfassung nach Regel 5.1(a)(ii) PCT bestanden.

M.H

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESSENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts FH990804PCT	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/EP 99/ 06312	Internationales Anmeldedatum (Tag/Monat/Jahr) 27/08/1999	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 22/09/1998

Anmelder

FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG... ET AL:

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.



Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.



Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das



in der internationalen Anmeldung in Schriftlicher Form enthalten ist.



zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.



bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.



bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.



Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.



Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. ☐ **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der Bezeichnung der Erfindung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der Zusammenfassung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1



wie vom Anmelder vorgeschlagen



keine der Abb.



weil der Anmelder selbst keine Abbildung vorgeschlagen hat.



weil diese Abbildung die Erfindung besser kennzeichnet.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

REC'D 20 NOV 2000



WIPO PCT

Aktenzeichen des Anmelders oder Anwalts FH990804PCT	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsbericht (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP99/06312	Internationales Anmeldedatum (Tag/Monat/Jahr) 27/08/1999	Prioritätsdatum (Tag/Monat/Tag) 22/09/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G07F7/10		
Anmelder FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG... et al.		

- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationale vorläufigen Prüfung beauftragte Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.
 - ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 10 Blätter.

- Dieser Bericht enthält Angaben zu folgenden Punkten:
 - I ☒ Grundlage des Berichts
 - II ☐ Priorität
 - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
 - IV ☐ Mangelnde Einheitlichkeit der Erfindung
 - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderische Tätigkeit und der gewerbliche Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
 - VI ☐ Bestimmte angeführte Unterlagen
 - VII ☐ Bestimmte Mängel der internationalen Anmeldung
 - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 06/04/2000	Datum der Fertigstellung dieses Berichts 16. 11. 00
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Kampka, A Tel. Nr. +49 89 2399 2244 

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1,2,4-20	ursprüngliche Fassung			
3,3a-3b	eingegangen am	02/08/2000	mit Schreiben vom	02/08/2000

Patentansprüche, Nr.:

1-18	eingegangen am	02/08/2000	mit Schreiben vom	02/08/2000
------	----------------	------------	-------------------	------------

Zeichnungen, Blätter:

1/4-4/4	ursprüngliche Fassung
---------	-----------------------

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen Behörde in der Sprache: , zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, dass das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, dass die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1 - 18
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1 - 18
	Nein: Ansprüche	
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1 - 18
	Nein: Ansprüche	

2. Unterlagen und Erklärungen
siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Art. 35(2) PCT hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf die folgenden Dokumente verwiesen:

D1: EP-A-0 313 967 (GAO GES AUTOMATION ORG) 3. Mai 1989 (1989-05-03)

D2: EP-A-0 654 919 (SIEMENS AG) 24. Mai 1995 (1995-05-24)

D3: W. RANKL & W. EFFING: 'Handbuch der Chipkarten' 10. Februar 1998
(1998-02-10) , CARL HANSER VERLAG , MÜNCHEN WIEN XP002127583
022759

Der wesentliche Unterschied zwischen dem Konzept der D1 und dem Konzept der Erfindung besteht darin, daß gemäß D1 die individuellen Kenndaten des Speichers 53 immer die gleichen sind, völlig unabhängig von der in die Karte 51 eingespeisten Zufallszahl. Bei der Erfindung ist es jedoch wesentlich, daß die Betriebsdaten der Schaltung eben von den Eingangsdaten der Schaltung abhängen. Dokument D1 offenbart keine Einrichtung zum Erfassen von Betriebsdaten der elektronischen Schaltung, die durch einen Betrieb der elektronischen Schaltung beeinflußt werden, wenn die elektronische Schaltung den Algorithmus ausführt. Darüberhinaus hängen bei D1 die individuellen Speicherdaten nicht von den Eingangsdaten, d.h. der Zufallszahl, welche vom Block Z in Fig. 11 zum Block RN übertragen wird, ab. Dokument D1 offenbart somit auch keine Einrichtung zum Erfassen von Betriebsdaten der elektronischen Schaltung (die Betriebsdaten der Einrichtung 60 in Fig. 11 werden nicht erfaßt, der Speicher 52 ist kein Element, das abhängig von Eingangsdaten in die Karte Ausgangsdaten aus der Karte erzeugt). D1 offenbart ferner nicht, daß die erfaßten Betriebsdaten der elektronischen Schaltung von dem Algorithmus, der durch die elektronische Schaltung ausgeführt wird, verwendet werden, da solche Betriebsdaten der elektronischen Schaltung gar nicht erfaßt werden.

Ausgehend von der D1 besteht die Aufgabe darin, ein Konzept zum verbesserten Schutz von elektronischen Schaltungen zu schaffen und somit eine

fälschungssichere Überprüfung der Authentizität solcher elektronischen Schaltungen und eine fälschungssichere Autorisierung eines Inhabers solcher elektronischer Schaltungen zu schaffen.

Diese Aufgabe wird erfindungsgemäß durch eine Vorrichtung nach Anspruch 1 bzw. ein Verfahren nach Anspruch 17 oder 18 gelöst.

Die in den unabhängigen Ansprüchen definierte Lösung beruht auf einer erfinderischen Tätigkeit: es werden nicht, wie in D1, individuelle Kenndaten irgendeiner elektronischen Schaltung verwendet, sondern die Betriebsdaten genau der elektronischen Schaltung, die abhängig von Eingangsdaten Ausgangsdaten erzeugt. Nach dem erfindungsgemäßen Konzept wird vom Speichern von irgendwelchen Kenndaten in einer Zentrale Abstand genommen.

D1 lehrt von der erfindungsgemäßen Lösung weg, weil hier die individuellen Kenndaten des Speichers immer die gleichen sind und deshalb zu Anfang abgespeichert werden können, während erfindungsgemäß die Betriebsdaten von den Eingangsdaten abhängen, so daß eine einmalige Abspeicherung der Betriebsdaten überhaupt keinen Sinn machen würde. D2 und D3 liegen vom Gegenstand der vorliegenden Erfindung noch weiter ab als D1. Zwar wird hier ausführlicher auf verschiedene Authentisierungsverfahren zwischen Sender und Empfänger eingegangen, jedoch gibt es keinerlei Anregung, bei Ausgangsdaten der Karte, die autorisiert werden soll, deren technologischen Betriebsverhalten hineinspielen zu lassen.

Zur gewerblichen Anwendbarkeit ist nichts einzuwenden.

Somit dürften die unabhängigen Ansprüche 1, 17 und 18 die in Artikel 33(1) PCT genannten Kriterien der Neuheit, erfinderischen Tätigkeit und gewerblichen Anwendbarkeit erfüllen. Die Ansprüche 2 - 16 betreffen vorteilhafte Ausgestaltungen und erfüllen daher ebenfalls die genannten Kriterien.

Der Anmelder beantragte die einteilige Fassung für Anspruch 1, weil seines Erachtens eine Abgrenzung gegenüber D1 zu einem schwerer verständlichen Anspruch führen würde. Da aus der ausführlichen Diskussion der D1 in der

Beschreibung klar ersichtlich ist, welche Merkmale des Anspruchs 1 aus dem Stand der Technik schon bekannt sind, wird gemäß den Richtlinien PCT/GL/3, III, 2.3a im vorliegenden Fall nicht auf der zweiteiligen Anspruchsfassung nach Regel 5.1(a)(ii) PCT bestanden.

- 3 -

Commerce, von Markus Kuhn und Ross Anderson, dargestellt worden ist, existieren viele Fälschungsverfahren, die weiterhin den anhaltenden Bedarf nach besseren Schutzmechanismen für Schaltungen und insbesondere für integrierte Schaltungen auf einer Chipkarte unterstreichen. Übliche Datenverschlüsselungsverfahren, die beispielsweise auf dem DES-Algorithmus basieren (DES Data Encryption Standard) oder die Prüfsummenalgorithmen umfassen, liefern zwar eine hohe Sicherheit, wenn der Verschlüsselungsschlüssel, der zusammen mit dem Krypto-Algorithmus eine Entschlüsselung ermöglicht, geheimgehalten wird. Prinzipiell ist es jedoch auch hier möglich, einen solchen Algorithmus, der in Form einer integrierten Schaltung auf einer Chipkarte hardware-mäßig integriert ist, anhand der Hardware-Implementation nachzuahmen, d. h. dessen Funktionalität beispielsweise mittels eines Computers zu simulieren.

~~Die Aufgabe der vorliegenden Erfindung besteht darin, ein Konzept zum verbesserten Schutz von elektronischen Schaltungen zu schaffen und somit eine fälschungssicherere Überprüfung der Authentizität solcher elektronischen Schaltungen und eine fälschungssicherere Autorisierung eines Inhabers solcher elektronischer Schaltungen zu schaffen.~~

Diese Aufgabe wird durch eine Vorrichtung nach Anspruch 1 und durch ein Verfahren nach Anspruch 17 oder 18 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß es zwar relativ einfach ist die Funktionalität eines Chips zu kopieren, daß es jedoch viel schwieriger ist, dessen Zeit- oder Leistungsverhalten nachzubilden. Eine Vorrichtung zum Liefern von Ausgangsdaten als Reaktion auf Eingangsdaten, um abhängig von den Ausgangsdaten die Authentizität der Vorrichtung zu bestimmen, umfaßt daher einerseits eine elektronische Schaltung zum Ausführen eines Algorithmus, der aus den Eingangsdaten die Ausgangsdaten erzeugt, ~~und andererseits eine Einrichtung zum Erfassen von~~

→ Seite 3a

- 3a -

Die EP 0 313 967 bezieht sich auf ein Verfahren zur Echtheitsprüfung eines Datenträgers mit integriertem Schaltkreis. Eine Karte enthält einen Speicher, der aus einem von außen zugänglichen und einem von außen nicht zugänglichen Bereich für die Speicherung von vertraulichen Informationen, z.B. einem Schlüssel, usw. besteht. Die Karte weist ferner einen Meßkreis für die Bestimmung der individuellen Kenndaten der Karte, wie z.B. der Programmierzeiten von E²PROM-Zellen des Speichers, auf. Der Meßschaltkreis ist mit dem Speicher verbunden und kann zusätzlich Verarbeitungseinrichtungen für die Aufarbeitung der gemessenen Daten aufweisen. Die Karte enthält ferner eine Verschlüsselungseinrichtung, die die individuellen Kenndaten der Speicherzelle sowie eine von einer Zentrale übermittelte Zufallszahl unter Verwendung eines ebenfalls im Speicher gespeicherten Schlüssels verschlüsselt, um einen verschlüsselten Ausgangswert zu erzeugen, welcher in einer Zentrale wieder mit einem entsprechenden Schlüssel entschlüsselt wird, so daß sich wieder die Zufallszahl einerseits und die individuellen Kenndaten des Speichers andererseits ergeben. Die individuellen Kenndaten des Speichers sind immer die gleichen, unabhängig von der in die Karte eingespeisten Zufallszahl. Die wieder entschlüsselte Zufallszahl wird mit der von der Zentrale zur Karte übermittelten Zufallszahl verglichen. Die ermittelten individuellen Kenndaten der Speicherzelle werden mit in der Zentrale abgespeicherten Kenndaten überprüft. Stimmen sowohl Zufallszahl als auch Kenndaten überein, so wird davon ausgegangen, daß die überprüfte Karte authentisch ist. Stimmt zwar die Zufallszahl überein, sind die individuellen Kenndaten aber unterschiedlich, so kann davon ausgegangen werden, daß eine gefälschte Karte vorliegt, deren Funktionalität der der authentischen Karte entspricht, die jedoch andere Kenndaten aufweist.

→ Seite 3b

- 3b -

~~Commerce, von Markus Kuhn und Ross Anderson, dargestellt~~
worden ist, existieren viele Fälschungsverfahren, die weiterhin den anhaltenden Bedarf nach besseren Schutzmechanismen für Schaltungen und insbesondere für integrierte Schaltungen auf einer Chipkarte unterstreichen. Übliche Datenverschlüsselungsverfahren, die beispielsweise auf dem DES-Algorithmus basieren (DES Data Encryption Standard) oder die Prüfsummenalgorithmen umfassen, liefern zwar eine hohe Sicherheit, wenn der Verschlüsselungsschlüssel, der zusammen mit dem Krypto-Algorithmus eine Entschlüsselung ermöglicht, geheimgehalten wird. Prinzipiell ist es jedoch auch hier möglich, einen solchen Algorithmus, der in Form einer integrierten Schaltung auf einer Chipkarte hardware-mäßig integriert ist, anhand der Hardware-Implementation nachzuahmen, d. h. dessen Funktionalität beispielsweise mittels eines Computers zu simulieren.

Die Aufgabe der vorliegenden Erfindung besteht darin, ein Konzept zum verbesserten Schutz von elektronischen Schaltungen zu schaffen und somit eine fälschungssicherere Überprüfung der Authentizität solcher elektronischen Schaltungen und eine fälschungssicherere Autorisierung eines Inhabers solcher elektronischer Schaltungen zu schaffen.

Diese Aufgabe wird durch eine Vorrichtung nach Anspruch 1 und durch ein Verfahren nach Anspruch 17 oder 18 gelöst.

Der vorliegenden Erfindung liegt die Erkenntnis zugrunde, daß es zwar relativ einfach ist die Funktionalität eines Chips zu kopieren, daß es jedoch viel schwieriger ist, dessen Zeit- oder Leistungsverhalten nachzubilden. Eine Vorrichtung zum Liefern von Ausgangsdaten als Reaktion auf Eingangsdaten, um abhängig von den Ausgangsdaten die Authentizität der Vorrichtung zu bestimmen, umfaßt daher einerseits eine elektronische Schaltung zum Ausführen eines Algorithmus, der aus den Eingangsdaten die Ausgangsdaten erzeugt, und andererseits eine Einrichtung zum Erfassen von

→ Seite 4

PATENTANSPRÜCHE

1. Vorrichtung (10) zum Liefern von Ausgangsdaten (12) als Reaktion auf Eingangsdaten (14), mit folgenden Merkmalen:

einer elektronischen Schaltung (16) zum Ausführen eines Algorithmus, um aus den Eingangsdaten (14) die Ausgangsdaten (12) zu erzeugen; und

einer Einrichtung (18) zum Erfassen von Betriebsdaten der elektronischen Schaltung (16), die durch einen Betrieb der elektronischen Schaltung (16) beeinflusst werden, wenn die elektronische Schaltung (16) den Algorithmus ausführt, wobei die Betriebsdaten von den Eingangsdaten abhängen,

wobei die Einrichtung (18) zum Erfassen von Betriebsdaten mit der elektronischen Schaltung (16) derart gekoppelt ist, daß die erfaßten Betriebsdaten der elektronischen Schaltung von dem Algorithmus, der durch die elektronische Schaltung (16) ausgeführt wird, verwendet werden, um die Ausgangsdaten (12) zu erzeugen, wodurch anhand der Ausgangsdaten die Authentizität der Vorrichtung (10) bestimmt wird.

2. Vorrichtung (10) nach Anspruch 1, bei der die Betriebsdaten aus der Gruppe ausgewählt sind, die Zeitdaten und Leistungsdaten umfaßt.
3. Vorrichtung (10) nach Anspruch 1 oder 2, bei der die elektronische Schaltung (16) und die Einrichtung (18) zum Erfassen als eine Einheit integriert sind.
4. Vorrichtung (10) nach einem der vorhergehenden Ansprüche, die in einer Smart Card oder einer PC-Card enthalten ist.

5. Vorrichtung (10) nach einem der vorhergehenden Ansprüche, bei der die elektronische Schaltung (16) angeordnet ist, um einen Krypto-Algorithmus auszuführen.
6. Vorrichtung (10) nach einem der Ansprüche 1 bis 4, bei der die elektronische Schaltung (16) angeordnet ist, um einen Prüfsummen-Algorithmus auszuführen.
7. Vorrichtung (10) nach Anspruch 5, bei der der Krypto-Algorithmus ein mehrstufiger Algorithmus ist, wobei die Betriebsdaten einer Algorithmus-Stufe als Eingangsdaten für die darauffolgende Algorithmus-Stufe verwendet werden.
8. Vorrichtung (10) nach einem der Ansprüche 1 bis 6, bei der die elektronische Schaltung (16) angeordnet ist, um nach einer vorbestimmten Ausführungszeit während der Ausführung des Algorithmus den Betrieb anzuhalten, und bei der die Einrichtung (18) zum Erfassen angeordnet ist, um Betriebsdaten zu der vorbestimmten Ausführungszeit in den Algorithmus einzuspeisen.
9. Vorrichtung (10) nach einem der Ansprüche 1 bis 3, bei der der Algorithmus derart gestaltet ist, daß er die Eingangsdaten (14) zunächst randomisiert, wodurch die Abhängigkeit der Betriebsdaten von den Eingangsdaten pseudozufällig ist.
10. Vorrichtung (10) nach Anspruch 9, bei der die Ausgangsdaten, die durch den Algorithmus erzeugt werden, lediglich die Betriebsdaten sind.
11. Vorrichtung (10) nach einem der Ansprüche 1 bis 4, bei der die elektronische Schaltung (16) zwei Teilschaltungen (16a, 16b) aufweist, die je einen Teil-Algorithmus ausführen, wobei der erste Teil-Algorithmus ein Test-

- 3 -

Algorithmus ist, dessen Betriebsdaten durch die Einrichtung (18) zum Erfassen erfaßt werden, und wobei der zweite Teil-Algorithmus ein Krypto-Algorithmus oder ein Prüfsummen-Algorithmus ist, wobei die Betriebsdaten des Test-Algorithmus in dem Krypto-Algorithmus verarbeitet werden.

12. Vorrichtung (10) nach Anspruch 11, bei der die zweite Teilschaltung (16a) angeordnet ist, um den DES-Algorithmus auszuführen, der n Stufen aufweist, und bei der die erste Teilschaltung (16b) angeordnet ist, um einen Test-Algorithmus auszuführen, der ebenfalls n Stufen aufweist, wobei die Eingangsdaten sowohl in die erste Stufe des DES-Algorithmus als auch in die erste Stufe des Test-Algorithmus einspeisbar sind, und wobei Daten, die in eine weitere Stufe des DES-Algorithmus einspeisbar sind, Ergebnisdaten der ersten Stufe des DES-Algorithmus und Betriebsdaten der ersten Stufe des Test-Algorithmus sind, während ein Ergebnis einer Stufe des Test-Algorithmus verworfen wird.
13. Vorrichtung (10) nach einem der vorhergehenden Ansprüche, bei der die Einrichtung zum Erfassen von Betriebsdaten eine Zeitmeßeinrichtung (18a) und eine Leistungsmeßeinrichtung (18b) aufweist, um die Zeit zu messen, die die elektronische Schaltung (16) zum Ausführen einer bestimmten Aufgabe benötigt, bzw. um die Leistung zu messen, die beim Ausführen der bestimmten Aufgabe verbraucht wird.
14. Vorrichtung (10) nach Anspruch 13, bei der die Leistungsmeßeinrichtung (18b) einen Widerstand, einen Kondensator und einen A/D-Wandler zum Messen der verbrauchten Leistung aufweist.
15. Vorrichtung (10) nach Anspruch 13 oder 14, bei der die Zeitmeßeinrichtung einen internen Taktgenerator auf-

weist.

16. Vorrichtung (10) nach einem der vorhergehenden Ansprüche, bei der die Einrichtung (18) zum Erfassen der Betriebsdaten einen Mustererkennungs-Algorithmus aufweist, um aus Leistungs- oder Zeitparametern der elektronischen Schaltung (16) die Betriebsdaten zu erzeugen.
17. Verfahren zum Überprüfen der Authentizität einer zu testenden Vorrichtung gegenüber einer Prüfvorrichtung, wobei die zu testende Vorrichtung und die Prüfvorrichtung jeweils eine elektronische Schaltung (16) zum Ausführen eines Algorithmus, der aus Eingangsdaten (14) Ausgangsdaten (12) erzeugt, und eine Einrichtung (18) zum Erfassen von Betriebsdaten, die durch einen Betrieb der elektronischen Schaltung (16) beeinflußt werden und von den Eingangsdaten abhängen, aufweisen, wobei sowohl bei der zu testenden Vorrichtung als auch bei der Prüfvorrichtung die Einrichtung (18) zum Erfassen der Betriebsdaten mit der elektronischen Schaltung (16) derart gekoppelt ist, daß die Betriebsdaten der elektronischen Schaltung durch den Algorithmus verwendet werden, um die Ausgangsdaten zu erzeugen, wobei das Verfahren folgende Schritte aufweist:

Auswählen (40) von Eingangsdaten;

Einspeisen (42) der Eingangsdaten in die zu testende Vorrichtung (10);

in der zu testenden Vorrichtung,

Ausführen des Algorithmus durch die elektronische Schaltung der zu testenden Vorrichtung, um aus den Eingangsdaten die Ausgangsdaten zu erzeugen,

Erfassen von Betriebsdaten der elektronischen

- 5 -

Schaltung, die durch einen Betrieb der elektronischen Schaltung beeinflußt werden, wenn die elektronische Schaltung den Algorithmus ausführt, wobei die Betriebsdaten von den Eingangsdaten abhängen, und wobei die erfaßten Betriebsdaten der elektronischen Schaltung von dem Algorithmus, der durch die elektronische Schaltung (16) ausgeführt wird, verwendet werden, um die Ausgangsdaten (12) zu erzeugen;

Einspeisen (42) der Eingangsdaten in die Prüfvorrichtung (10);

in der Prüfvorrichtung,

Ausführen des Algorithmus durch die elektronische Schaltung der Prüfvorrichtung, um aus den Eingangsdaten die Ausgangsdaten zu erzeugen,

Erfassen von Betriebsdaten der elektronischen Schaltung, die durch einen Betrieb der elektronischen Schaltung beeinflußt werden, wenn die elektronische Schaltung den Algorithmus ausführt, wobei die Betriebsdaten von den Eingangsdaten abhängen, und wobei die erfaßten Betriebsdaten der elektronischen Schaltung von dem Algorithmus, der durch die elektronische Schaltung (16) ausgeführt wird, verwendet werden, um die Ausgangsdaten (12) zu erzeugen;

Vergleichen (44) der Ausgangsdaten der zu testenden Vorrichtung mit den Ausgangsdaten der Prüfvorrichtung; und

Bejahen (46) der Authentizität der zu testenden Vorrichtung gegenüber der Prüfvorrichtung, wenn die Ausgangsdaten übereinstimmen, derart, daß eine Authentizität lediglich dann bejaht wird, wenn die Betriebsdaten der zu testenden Vorrichtung und der Prüfvorrichtung entsprechend sind.

18. Verfahren zum verschlüsselten Übertragen von Informationen von einem ersten zu einem von dem ersten Ort entfernten zweiten Ort, mit folgenden Merkmalen:

Erzeugen (50) eines Zufallsworts;

Einspeisen (52) des Zufallsworts in eine erste Vorrichtung, die nach einem der Ansprüche 1 bis 16 ausgeführt ist und an dem ersten Ort angeordnet ist;

Erzeugen (54) der Ausgangsdaten der ersten Vorrichtung, die von den Betriebsdaten der ersten Vorrichtung abhängen, durch Ausführen eines Algorithmus durch die elektronische Schaltung der ersten Vorrichtung, um aus den Eingangsdaten die Ausgangsdaten zu erzeugen, wobei Betriebsdaten der elektronischen Schaltung erfaßt werden, die durch einen Betrieb der elektronischen Schaltung beeinflußt werden, wenn die elektronische Schaltung den Algorithmus ausführt, wobei die Betriebsdaten von den Eingangsdaten abhängen, und wobei die erfaßten Betriebsdaten der elektronischen Schaltung von dem Algorithmus, der durch die elektronische Schaltung ausgeführt wird, verwendet werden, um die Ausgangsdaten zu erzeugen;

Verschlüsseln (56) der Informationen mit den erzeugten Ausgangsdaten als Schlüssel;

Übertragen (58) der verschlüsselten Informationen und des Zufallsworts von dem ersten Ort zu dem zweiten Ort;

Einspeisen (62) des Zufallsworts in eine zweite Vorrichtung, die nach einem der Ansprüche 1 bis 16 ausgeführt ist und an dem zweiten Ort positioniert ist;

Erzeugen (64) der Ausgangsdaten der zweiten Vorrichtung, die von den Betriebsdaten der zweiten Vorrichtung abhängen;

gen, durch Ausführen des Algorithmus durch die elektronische Schaltung der zweiten Vorrichtung, um aus den Eingangsdaten die Ausgangsdaten zu erzeugen, wobei Betriebsdaten der elektronischen Schaltung erfaßt werden, die durch einen Betrieb der elektronischen Schaltung beeinflußt werden, wenn die elektronische Schaltung den Algorithmus ausführt, wobei die Betriebsdaten von den Eingangsdaten abhängen, und wobei die erfaßten Betriebsdaten der elektronischen Schaltung von dem Algorithmus, der durch die elektronische Schaltung ausgeführt wird, verwendet werden, um die Ausgangsdaten zu erzeugen;

Entschlüsseln (66) der verschlüsselten Informationen unter Verwendung der Ausgangsdaten der zweiten Vorrichtung als Schlüssel,

wobei die entschlüsselten Informationen dann den ursprünglichen Informationen vor dem Verschlüsseln entsprechen, wenn die Betriebsdaten der ersten Vorrichtung an dem ersten Ort den Betriebsdaten der zweiten Vorrichtung an dem zweiten Ort entsprechen.